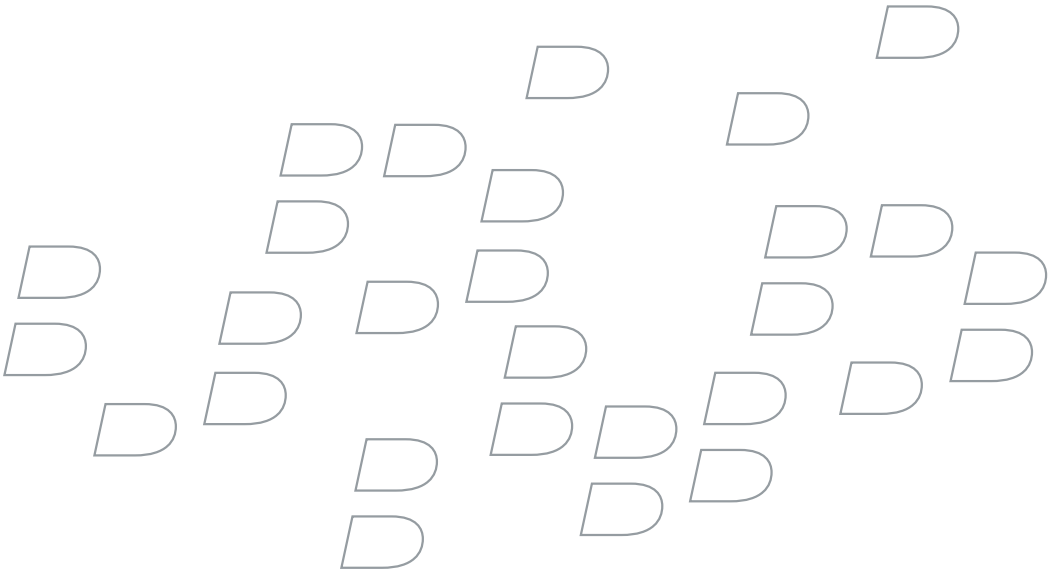

BlackBerry Enterprise Server

All released versions (4.1.3 and earlier)

Policy Reference Guide (Version 12)

BlackBerry Enterprise Server All released versions (4.1.3 and earlier) Policy Reference Guide

Last modified: 22 March 2007

Part number: 6199802 Version 12

Send us your comments on product documentation: https://www.blackberry.com/DocsFeedback.

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 2007.

Contents

1

New IT policy rules

New in this release

Policy Group	IT policy rule	Default setting	BlackBerry Enterprise Server software (minimum requirement)
C/MIME	Disable Notes Native Encryption Forward And Reply	False	4.1.3
Location Based Services (renamed from BlackBerry Maps)	Enable Enterprise Location Tracking	False	4.1.3
	Enterprise Location Tracking User Prompt Message	Your location is now being tracked at the server.	4.1.3
	Enterprise Location Tracking Interval	False	4.1.3

Importing IT policy rules without the minimum BlackBerry Enterprise Server software required

Visit www.blackberry.com/btsc to view the article KB-05439 "How To - Import IT policy rules for BlackBerry Device Software 4.2" for information about adding new IT policy rules to a BlackBerry Enterprise Server version earlier than the minimum requirement.

2

IT policy rules

Assign IT policy rule values in the IT policy that reflect the needs of the user(s) assigned to that IT policy and your corporate IT policy requirements. For example, you can create an IT policy, set the IT policy rules in that IT policy for executive functionality and security requirements, add the desired executives to a group, and assign the IT policy to the group.

See the *BlackBerry Enterprise Server System Administration Guide* for more information on how to create an IT policy, set an IT policy rule, and assign an IT policy to a user or group.

Understanding IT policy rule names and groups

The BlackBerry® Manager groups the IT policy rules by common properties or by the application they can control. Research In Motion (RIM) intends the name of most IT policy rules to indicate how you can use that rule to change default BlackBerry device and BlackBerry Desktop Software functionality.

RIM intends most IT policy rules to control multiple BlackBerry devices and desktop software settings in your organization.

Applying WLAN, VPN, and VoIP IT policy rules

Some IT policy rules configure a global or a unique value for a BlackBerry device that you administer on a wireless LAN. You should assign unique rules to one BlackBerry device and to one user only. See the *BlackBerry Enterprise Server Implementation Guide for Wireless LAN* for more information on IT policy rules that appear in the WLAN, VPN and VoIP policy groups. Those IT policy rules are currenly documented in the *BlackBerry Enterprise Server Implementation Guide for Wireless LAN* only.

Applying IT policy rules to BlackBerry Connect and BlackBerry Built-In devices

If the BlackBerry Enterprise Server™ pushes an IT policy rule that the BlackBerry Connect™ Transport Stack is aware of to the BlackBerry device, the transport stack reports the IT policy rule to the BlackBerry Connect application. The transport stack can implement a specific subset of the IT policy rules internally. You must use the BlackBerry Connect application to implement as many of the remaining IT policy rules as possible.

BlackBerry Built-In™ devices can support all documented IT policy rules, depending on the specific BlackBerry Built-In implementation.

IT policy rule descriptions

Notes: The minimum requirements indicated in the following tables apply to wireless IT policy rules only. This document does not include minimum requirements for IT policy rules that you can implement using the BlackBerry Desktop Software with the BlackBerry Enterprise Server versions that do not support wireless IT policy. The minimum requirements for BlackBerry Enterprise Server Software indicate the

Any exceptions to a policy rule are listed by the BlackBerry Enterprise Server platform to which they apply, below the most commonly applicable information for that policy rule.

See the *BlackBerry Enterprise Solution Security Acronym Glossary* for the full terms substituted by the acronyms in this document.

Location Based Services policy group

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Disable BlackBerry Maps	Specify whether or not the BlackBerry Maps functionality is disabled on the BlackBerry device.	False	Java® based	4.0	4.0.6	–	–
Enable Enterprise Location Tracking	Specify whether or not to turn on Enterprise Location Tracking on the BlackBerry device.	False	Java based	4.2.1	4.1.3	–	Set this rule to True to require the BlackBerry device to report its location to the BlackBerry Enterprise Server at regular intervals.
Enterprise Location Tracking User Prompt Message	Specify the message that the BlackBerry device displays to notify the BlackBerry device user when Enterprise Location Tracking is enabled.	Your location is now being tracked at the server.	Java based	4.2.1	4.1.3	–	–
Enterprise Location Tracking Interval	Type the interval, in minutes, after which a BlackBerry device reports its location to the BlackBerry Enterprise Server.	15	Java based	4.2.1	4.1.3	–	The range permitted is 15 to 60 minutes.

BlackBerry Messenger policy group

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Disable BlackBerry Messenger	Specify whether or not the BlackBerry Messenger™ is turned off on the BlackBerry device.	False	Java based	3.6	4.0.2	–	–
Messenger Audit Email Address	Specify the address to which the BlackBerry Messenger audit reports are sent.	–	Java based	4.0	4.0.2	–	If no address is specified, the BlackBerry Messenger turns off auditing and does not send reports.
Messenger Audit Max Report Interval	Specify the interval, in hours, after which a new BlackBerry Messenger audit report is sent whether or not there is new data.	168	Java based	4.0	4.0.2	–	–
Messenger Audit Report Interval	Specify the interval, in hours, after which the BlackBerry Messenger sends a new audit report if there is new data.	24	Java based	4.0	4.0.2	–	Set to a shorter interval to manage BlackBerry device memory.
Messenger Audit UID	Specify the unique identifier (UID) of the service book to use when sending the BlackBerry Messenger audit reports.	–	Java based	4.0	4.0.2	–	If you leave this IT policy rule blank, the first available encrypted message service is used.

Bluetooth policy group

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Allow Outgoing Calls	Specify whether or not the user can place outgoing phone calls from a Bluetooth®-enabled BlackBerry device. • **0**: always • **1**: only when the BlackBerry device is unlocked • **2**: never	0	Java based	4.0.2	4.0.2	–	–
Disable Address Book Transfer	Specify whether or not the BlackBerry device can exchange address book data with supported Bluetooth-enabled devices.	False	Java based	4.1	4.0.3	–	–
Disable Bluetooth	Specify whether or not Bluetooth support is turned off on the BlackBerry device.	False	Java based	3.8	4.0	4.0	If the Bluetooth wireless radio is active when the BlackBerry device receives this IT policy rule, the BlackBerry device must be reset for the change to take effect.
BlackBerry Enterprise Server for Novell® GroupWise® exceptions:			–	4.0	–	–	–
Disable Desktop Connectivity	Specify whether or not the BlackBerry device can use Bluetooth technology to connect to the BlackBerry Desktop Manager.	True	Java based	4.1	4.0.3	–	–
Disable Dial-Up Networking	Specify whether or not the Bluetooth-enabled BlackBerry device can use the Bluetooth Dial-Up Networking Profile (DUN).	False	Java based	4.2	4.0.6	–	–

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Disable Discoverable Mode	Specify whether or not discoverable mode can be enabled on Bluetooth-enabled BlackBerry devices.	False	Java based	4.0.2	4.0.2	—	—
Disable File Transfer	Specify whether or not the Bluetooth-enabled BlackBerry device can exchange files with compatible Bluetooth OBject EXchange (OBEX) devices.	False	Java based	4.2	4.0.6	—	—
Disable Handsfree Profile	Specify whether or not the user can turn on or turn off the Bluetooth Hands Free Profile (HFP) on the Bluetooth-enabled BlackBerry device.	False	Java based	3.8	4.0	4.0	The BlackBerry device requires the Bluetooth HFP to enable wireless voice capabilities with most car kits and some headsets.
BlackBerry Enterprise Server for Novell GroupWise exceptions:			—	—	4.0	—	—
Disable Headset Profile	Specify whether or not the user can turn on or turn off the Bluetooth Headset Profile (HSP) on the Bluetooth-enabled BlackBerry device.	False	Java based	3.8	4.0	4.0	The BlackBerry device requires the Bluetooth HSP to enable wireless voice capabilities with most headsets and some car kits.
BlackBerry Enterprise Server for Novell GroupWise exceptions:			—	4.0	—	—	—
Disable Pairing	Specify whether or not the Bluetooth-enabled BlackBerry device can establish a relationship—or pair— with another Bluetooth-enabled device.	False	Java based	3.8	4.0	4.0	After the BlackBerry device establishes a pairing with a supported Bluetooth-enabled device (for example, a headset), you can use this IT policy rule to prevent the BlackBerry device from establishing any subsequent pairings.

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
BlackBerry Enterprise Server for Novell GroupWise exceptions:			—	4.0	—	—	—
Disable Serial Port Profile	Specify whether or not the Bluetooth-enabled BlackBerry device can use the Bluetooth Serial Port Profile (SPP).	False	Java based	3.8	4.0	4.0	The BlackBerry device requires the Bluetooth SPP for establishing a serial connection between the BlackBerry device and a Bluetooth-enabled device using a serial port interface.
BlackBerry Enterprise Server for Novell GroupWise exceptions:			—	4.0	—	—	—
Disable Wireless Bypass	Specify whether or not the Bluetooth-enabled BlackBerry device can perform wireless bypass using Bluetooth technology.	True	Java based	4.1	4.0.3	—	—
Require Encryption	Specify whether or not the Bluetooth-enabled BlackBerry device uses Bluetooth encryption on all connections.	False	Java based	4.1.0	4.0.4	—	If you set this IT policy rule to True to require Bluetooth encryption on all connections, you might restrict compatibility with other Bluetooth devices.
Require LED Connection Indicator	Specify whether or not the Bluetooth-enabled BlackBerry device LED flashes when the BlackBerry device is connected to another Bluetooth-enabled device.	False	Java based	4.2	4.0.6	—	—
Require Password for Enabling Bluetooth Support	Specify whether or not the Bluetooth-enabled BlackBerry device password is required to enable Bluetooth support.	False	Java based	4.1.0	4.0.3	—	**Rule dependency:** The BlackBerry device uses this IT policy rule only if the Password Required rule is set to True.

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Require Password for Discoverable Mode	Specify whether or not a BlackBerry device password is required to enable the BlackBerry device to enter discoverable mode.	False	Java based	4.1.0	4.0.3	—	**Rule dependency:** The BlackBerry device uses this IT policy rule only if the Password Required rule is set to True.

Bluetooth Smart Card Reader policy group

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Force Erase All Keys on BlackBerry Disconnected Timeout	Specify whether or not the secure pairing keys for the current BlackBerry device and computer connections to the BlackBerry Smart Card Reader are cleared when the BlackBerry disconnected timeout fires.	False. The secure pairing information is not deleted from the BlackBerry device or the desktop computer.	Java based	BlackBerry Smart Card Reader Version 1.5	4.0.5	—	The user can enable this feature on the BlackBerry device. If you set this IT policy rule to True, the user cannot disable this feature on the BlackBerry device. **Related IT policy rule:** Maximum BlackBerry Disconnected Timeout

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Maximum BlackBerry Disconnected Timeout	Specify the maximum time, in seconds, after the BlackBerry device and the BlackBerry Smart Card Reader close the Bluetooth connection between them that the disconnected timeout fires. If you do not specify a disconnected timeout value, the user can choose any disconnected timeout value or set the Disconnected Timeout value to None on the BlackBerry device to disable this feature.	None. The secure pairing information is not deleted from the BlackBerry device.	Java based	4.0 BlackBerry Smart Card Reader Version 1.0	4.0.2	–	If you specify a disconnected timeout value, the user cannot disable the timeout, but can decrease the Disconnected Timeout field value from that value on the BlackBerry device. **Related IT policy rule**: Force Erase All Keys on BlackBerry Disconnected Timeout
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported	Not supported	Not supported	–	–
Maximum BlackBerry Bluetooth Traffic Inactivity Timeout	Specify the maximum time, in minutes, of secure Bluetooth traffic inactivity permitted between the BlackBerry Smart Card Reader and the BlackBerry device before the secure pairing information is removed from the BlackBerry device and the BlackBerry Smart Card Reader. **Note**: Activity is any secure packet other than the connection heartbeat sent or received by the BlackBerry device and the BlackBerry Smart Card Reader. The user cannot disable the inactivity timeout, but can decrease the Inactivity Timeout field value from that value on the BlackBerry device.	None. The secure pairing information is not deleted from the BlackBerry device.	Java based	4.0	4.0.2	–	If you specify a BlackBerry Bluetooth traffic inactivity timeout value, the user can choose any inactivity timeout value or set the Inactivity Timeout field value to None on the BlackBerry device to disable this feature.

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported	Not supported	Not supported	–	–
Maximum BlackBerry Long Term Timeout	Specify the maximum time, in hours, after the BlackBerry device and the BlackBerry Smart Card Reader establish the secure pairing information between them, that the BlackBerry device and the BlackBerry Smart Card Reader remove their secure pairing information. If you specify a long term timeout value, the user cannot disable the timeout, but can decrease the Long Term Timeout field value from that value on the BlackBerry device. If you do not specify a long term timeout value, the user can choose any disconnected timeout value or set the Long Term Timeout field value to None on the BlackBerry device to disable this feature.	False	Java based	4.0	4.0.2	–	**Related IT policy rules**: Maximum BlackBerry Bluetooth Traffic Inactivity Timeout
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported	Not supported	Not supported	–	–
Maximum Bluetooth Range	Specify the maximum power range as a value between 30% (shortest range) and 100% (longest range), that the BlackBerry Smart Card Reader uses to send Bluetooth packets.	100%	Java based	4.0 BlackBerry Smart Card Reader Version 1.0	4.0.3	–	Set a longer range to enable the BlackBerry device or the computer to communicate with the BlackBerry Smart Card Reader over a greater distance
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported	Not supported	Not supported	–	–

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Maximum Connection Heartbeat Period	Specify the maximum heartbeat period, in seconds. Each heartbeat period, the paired BlackBerry device or computer sends a heartbeat which the BlackBerry Smart Card Reader acknowledges. If either side fails to send or acknowledge a heartbeat in the maximum heartbeat period, the BlackBerry device or computer closes the Bluetooth connection. **Note**: When the connection closes, the disconnected timer starts if you or the user enabled that feature on the BlackBerry device or computer. The BlackBerry device or computer clears the secure pairing keys when the disconnected timer expires. If you do not set this IT policy rule, the user can choose any period or set the Connection Heartbeat Period field value to None on the BlackBerry device or computer to disable the heartbeat period. **Rule dependency**: You can use the Maximum BlackBerry Disconnected Timeout and Maximum PC Disconnected Timeout IT policy rules to specify the BlackBerry device and computer disconnected timers.	None. The heartbeat period is disabled.	Java based	BlackBerry Smart Card Reader Version 1.0	4.0.2	–	Use this IT policy rule to prevent an attacker from using a low-level Bluetooth heartbeat to keep the Bluetooth connection open between the BlackBerry device or computer, and the BlackBerry Smart Card Reader and the secure pairing keys present, for an extended period after the connection should be terminated. If you set this IT policy rule, the user cannot disable the heartbeat, but can decrease the Connection Heartbeat Period field value from that period on the BlackBerry device or computer. **Warning**: If you set this IT policy rule to a low heartbeat period (None, 1, 2, or 5 seconds), the increased Bluetooth traffic decreases the battery life of the BlackBerry device and BlackBerry Smart Card Reader.

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported	Not supported	Not supported	–	–
Maximum Number of BlackBerry Transactions	Specify the maximum number of transactions (smart card–related operations) that the BlackBerry device and the BlackBerry Smart Card Reader can send and receive before the secure pairing information is removed from the BlackBerry device. **Note**: A transaction is any request and response set of packets other than a connection heartbeat. If you do not specify a maximum number of BlackBerry transactions, the user can choose any number of BlackBerry transactions or set the Number of Transactions field value to None on the BlackBerry device to disable this feature.	None. The secure pairing information is not deleted from the BlackBerry device.	Java based	4.0	4.0.2	–	If you specify a maximum number of BlackBerry transactions, the user cannot disable the secure pairing wipe, but can decrease the Number of Transactions field value from that value on the BlackBerry device.
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported	Not supported	Not supported	–	–

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Maximum Number of PC Pairings	Specify the maximum number of computers that can pair with the BlackBerry Smart Card Reader.	—	—	BlackBerry Smart Card Reader Version 1.5	4.0.5	—	If you specify a maximum number of PC pairings while computers are paired with the BlackBerry Smart Card Reader, the BlackBerry Smart Card Reader disconnects and removes the pairings of the last computer(s) to connect that exceed the maximum number permitted.
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported	Not supported	Not supported	—	—

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Maximum Number of PC Transactions	Specify the maximum number of transactions (smart card–related operations) that the computer and the BlackBerry Smart Card Reader can send and receive between them before the secure pairing information is removed from the computer and the BlackBerry Smart Card Reader. **Note**: A transaction is any request and response set of packets other than a connection heartbeat. If you do not specify a maximum number of PC transactions,the user can choose any number of PC transactions or set the Number of Transactions field value to None in the BlackBerry Smart Card Reader Options on the computer to disable this feature.	–	–	BlackBerry Smart Card Reader Version 1.5	4.0.5	–	If you specify a maximum number of PC transactions, the user cannot change the number of transactions, but can decrease the Number of Transactions field value from that value in the BlackBerry Smart Card Reader Options on the computer.
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported	Not supported	Not supported	–	–

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Maximum PC Bluetooth Traffic Inactivity Timeout	Specify the maximum time, in minutes, of secure Bluetooth traffic inactivity permitted between the BlackBerry Smart Card Reader and the computer before the secure pairing information is removed from the computer and the BlackBerry Smart Card Reader. **Note**: Activity is any secure packet other than the connection heartbeat sent or received by the BlackBerry device and the BlackBerry Smart Card Reader. If you do not specify a long term timeout value, the user can choose any inactivity timeout value or set the Inactivity Timeout field value to None in the BlackBerry Smart Card Reader Options on the computer to disable this feature.	None. The secure pairing information is not deleted from the desktop computer.	–	BlackBerry Smart Card Reader Version 1.5	4.0.5	–	If you specify a long term timeout value, the user cannot disable the inactivity timeout, but can decrease the Inactivity Timeout field value from that value in the BlackBerry Smart Card Reader Options on the computer.
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported	Not supported	Not supported	–	–

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Maximum PC Disconnected Timeout	Specify the maximum time, in seconds, after the computer and the BlackBerry Smart Card Reader close the Bluetooth connection between them that the secure pairing information for that dropped connection is removed from the computer and the BlackBerry Smart Card Reader. If you do not specify a maximum PC disconnected timeout value, the user can choose any maximum PC disconnected timeout or set the Disconnected Timeout field value to None in the BlackBerry Smart Card Reader Options on the computer to disable this feature.	—	—	BlackBerry Smart Card Reader Version 1.5	4.0.5	—	If you specify a maximum PC disconnected timeout value, the user cannot disable the PC disconnected timeout, but can decrease the Disconnected Timeout field value in the BlackBerry Smart Card Reader Options on the computer.
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported	Not supported	Not supported	—	—

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Maximum PC Long Term Timeout	Specify the maximum time, in hours, after the computer and the BlackBerry Smart Card Reader establish the secure pairing information between them that the computer and the BlackBerry Smart Card Reader remove their secure pairing information. If you do not specify a long term timeout value, the user can choose any disconnected timeout value or set the Long Term Timeout field value to None in the BlackBerry Smart Card Reader Options on the computer to disable this feature.	–	–	BlackBerry Smart Card Reader Version 1.5	4.0.5	–	If you specify a long term timeout value, the user cannot disable the timeout, but can decrease the Long Term Timeout field value from that value in the BlackBerry Smart Card Reader Options on the computer. **Related IT policy rule**: Maximum PC Inactivity Timeout
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported	Not supported	Not supported	–	–
Maximum Smart Card Not Present Timeout	Specify the maximum time, in seconds, after the user removes the smart card from the BlackBerry Smart Card Reader that the secure pairing information is removed from the BlackBerry device and the BlackBerry Smart Card Reader. If you do not specify a smart card not present value, the user cannot disable the smart card not present timeout, but can decrease the Card Not Present Timeout field value from that value on the BlackBerry device.	None. The Bluetooth pairing information is not deleted from the BlackBerry device.	Java based	4.0	4.0.2	–	If you specify a smart card not present timeout value, the user can choose any smart card not present timeout value or set the Card Not Present Timeout field value to None on the BlackBerry device to disable this feature.
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported	Not supported	Not supported	–	–

Browser policy group

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Allow IBS Browser	Specify whether or not the Internet Browsing Service (IBS) browser icon appears on the BlackBerry device when the service provider provisions the IBS browser with the appropriate service books present.	True	Java based	4.0	4.0.1	4.0 (internal)	Set this IT policy rule to False to hide the IBS browser icon.
Disable Auto Synchronization in Browser	Specify whether or not the user can set auto synchronization intervals in the bookmarks in the BlackBerry Browser.	False	Java based	4.2	4.0.6	–	–
Disable Java Script in Browser	Specify whether or not the BlackBerry Browser can execute JavaScript™ scripts.	False	Java based	4.0	4.0	4.0 (internal)	–
Download Images URL	Specify a URL for a web site that lists additional images for the BlackBerry device.	–	Java based	4.1.0	4.0.3	–	–
Download Themes URL	Specify a URL for a web site that lists additional themes for the BlackBerry device.	–	Java based	4.1.0	4.0.3	–	–
Download Tunes URL	Specify a URL for a web site that lists additional tunes for the BlackBerry device.	–	Java based	4.1.0	4.0.3	–	–
MDS Browser BSM Enabled	Specify whether or not the Browser Session Manager (BSM) is enabled.	True	Java based	4.0.2	4.0.2	4.0 (internal)	The BSM is designed to improve BlackBerry Browser performance by helping BlackBerry MDS use the BlackBerry Browser cache.

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
MDS Browser Domains	Specify a comma-separated list of URL domains that the BlackBerry device should retrieve using the MDS Browser.	–	Java based	4.2	4.0.6	–	–
MDS Browser HTML Tables Enabled	Specify whether or not HTML tables are enabled in the BlackBerry Browser.	False	Java based	4.0.2	4.0.2	4.0 (internal)	–
MDS Browser JavaScript Enabled	Specify whether or not JavaScript is enabled in the BlackBerry Browser.	False	Java based	4.0.2	4.0.2	4.0 (internal)	Set this IT policy rule to True to properly render web pages that use JavaScript on the BlackBerry device.
MDS Browser Style Sheets Enabled	Specify whether or not style sheets are enabled in the BlackBerry Browser.	False	Java based	4.0.2	4.0.2	4.0 (internal)	–
MDS Browser Title	Specify the name that appears on the Home screen for the BlackBerry Browser icon.	BlackBerry Browser	Java based	3.6	4.0	4.0 (internal)	–
BlackBerry Enterprise Server for Microsoft® Exchange exceptions:			–	–	3.6	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			–	4.0	–	–	–
MDS Browser Use Separate Icon	Specify whether or not the BlackBerry device user can access the BlackBerry MDS Browser from a separate icon on the home screen.	False	Java based	4.2	4.0.6	–	–

Camera policy group

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Disable Camera	Specify whether or not the camera functionality is disabled on the BlackBerry device.	False	Java based	4.2	4.0.6	–	–

Certificate Sync policy group

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Default CRL Server URL	Specify the URL of the default CRL server used on the desktop.	–	–	–	3.6 or earlier (S/MIME Support Package version 1.5 or later)	–	This IT policy rule is obsolete in BlackBerry Enterprise Server version 4.0 and later.
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			Not supported	Not supported	Not supported	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported	Not supported	Not supported	–	–
Default LDAP Server URL	Specify the URL of the default LDAP server used on the desktop.	–	–	–	3.6 or earlier (S/MIME Support Package version 1.5 or later)	–	This IT policy rule is obsolete in BlackBerry Enterprise Server version 4.0 and later.
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			Not supported	Not supported	Not supported	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported	Not supported	Not supported	–	–
Default OCSP Server URL	Specify the URL of the default OCSP server used on the desktop.	–	–	–	3.6 or earlier (S/MIME Support Package version 1.5 or later)	–	This IT policy rule is obsolete in BlackBerry Enterprise Server version 4.0 and later.

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			Not supported	Not supported	Not supported	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported	Not supported	Not supported	–	–
Random Source URL	Specify a URL (for example, for a white noise machine) that produces truly random data. If the S/MIME Support Package version 4.0 or later is turned on and installed on the BlackBerry device, the BlackBerry Certificate Synchronization Manager in the BlackBerry Desktop Software can use the URL to retrieve random data to add to the BlackBerry device's random pool.	–	–	– BlackBerry Desktop Software version 4.0 S/MIME Support Package version 4.0 or later	–	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported	Not supported	Not supported	–	–

CMIME application policy group

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Allow Auto Attachment Download	Specify whether or not supported BlackBerry devices can automatically download supported attachments from received messages using the Attachment Service.	False	Java based	4.2	4.0.6	–	If you set this IT policy rule to True, users can use the auto attachment download message option on their BlackBerry devices if the Attachment Service is installed, running, and connected to the BlackBerry Enterprise Server using an attachment connector.
Attachment Viewing	Enables BlackBerry device users to view supported attachments on the BlackBerry device.	True	Java based	4.2	4.0.6	–	The BlackBerry device can use this IT policy rule if the Attachment Service is installed, running, and connected to the BlackBerry Enterprise Server using an attachment connector.
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	3.6.1	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Java based only	4.0	–	–	–

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Disable Notes Native Encryption Forward And Reply	Specify whether or not a BlackBerry device user can forward and reply to received IBM Lotus Notes encrypted messages on their BlackBerry devices. By default, a BlackBerry device user with support for reading IBM Lotus Notes encrypted messages enabled on the BlackBerry device can forward or reply to an encrypted message that the BlackBerry device has received, decrypted, and decompressed. The BlackBerry Enterprise Server for IBM Lotus Domino decrypts the message before the BlackBerry device sends the message to the recipient as plain text.	False	Java based	4.2.1	4.1.3	–	If you set this rule to True, BlackBerry device users cannot forward or reply to received IBM Lotus Notes encrypted messages on their BlackBerry devices.
Enable Wireless Message Reconciliation	Specify whether or not wireless message reconciliation functionality is supported on the BlackBerry device.	–	Java based or C++-based	3.6 (Java based BlackBerry device) or 2.6 (C++-based BlackBerry device)	4.0	1.2 2.0 2.1 4.0 (internal)	If you set this IT policy rule to True, or if it is not part of the IT policy to which you assigned the user, wireless message reconciliation is enabled on the BlackBerry device by default. Wireless message reconciliation must also be enabled on the BlackBerry Enterprise Server to function.
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	3.6	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Java based only	4.0	–	–	–

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Keep Message Duration	Specify the maximum length of time, in days, for which the BlackBerry device keeps messages. The permitted range is 0 to 180 days.	30 days	Java based	4.2	4.0.6	–	**Note**: Set this IT policy rule to -1 to keep messages on the BlackBerry device indefinitely.
Keep Saved Message Duration	Specify the maximum length of time, in days, for which the BlackBerry device keeps saved messages. The permitted range is 0 to 180 days.	90 days	Java based	4.2	4.0.6		**Note**: Set this IT policy rule to -1 to keep saved messages on the BlackBerry device indefinitely.
Prepend Disclaimer	Type a disclaimer to appear at the beginning of all email messages that the user composes and sends using the BlackBerry device.	–	Java based	4.1.2	4.0.5	–	–
Maximum Native Attachment MFH total attachment size	Specify the total size of all native attachments that can be uploaded from the BlackBerry device. The permitted range is 0 to 5 MB (in bytes).	5 MB	Java based	4.2	4.0.6	–	–
Maximum Native Attachment MFH attachment size	Specify the maximum size of a Native Attachment that can be uploaded from the BlackBerry device. The permitted range is 0 to 3 MB (in bytes).	3 MB	Java based	4.2	4.0.6	–	–

Common policy group

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
BlackBerry Server Version	Specify the BlackBerry Enterprise Server version number that is sent to the BlackBerry device. **Note**: Where applicable, if this IT policy rule is not set, the BlackBerry device uses the settings specified by other Application Control rules, or by software configurations defined in the BlackBerry device Configuration Tool. If no Application Control data exists, then the BlackBerry device uses split-pipe connections through the firewall.	—	Java based or C++-based	4.0 (Java based BlackBerry device) or 2.7 (C++-based BlackBerry device)	4.0 only (This IT policy rule was made obsolete by version 4.1.)	4.0	Set this IT policy rule to 4.0 to support Application Control features.
Confirm On Send	Specify whether or not the BlackBerry device requires users to confirm before sending a message, PIN message, Short Message Service (SMS) message, or Multimedia Messaging Service (MMS) message.	—	Java based or C++-based	4.0 (Java based BlackBerry device) or 2.7 (C++-based BlackBerry device)	4.0	4.0	Use this IT policy rule to customize a confirmation message. If this IT policy rule is not set, the confirmation dialog does not display.
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			—	—	—	—	—
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Java based only	4.0	—	—	—
Disable Kodiak PTT	Specify whether or not Kodiak Instant Calling™ , or Push to Talk (PTT), functionality is available on supported BlackBerry devices.	False	Java based	4.2	4.0.6	—	—

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Disable MMS	Specify whether or not MMS messaging is permitted on the BlackBerry device. **Note**: To block incoming MMS messages, set the Firewall Block Incoming Messages IT policy rule in the Security Policy Group.	False	Java based	4.0	4.0	4.0	Set this IT policy rule to True to hide the MMS functionality on the BlackBerry device.
Disable Voice-Activated Dialing	Specify whether or not voice-activated dialing functionality is available on the BlackBerry device	False	Java based	4.2	4.0.6	–	–
IT Policy Notification	Specify whether or not the BlackBerry device displays warnings of IT policy changes to the user.	False	Java based or C++-based	4.0 (Java based BlackBerry device) or 2.7 (C++-based BlackBerry device)	4.0	4.0	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Java based only	4.0	–	–	–
Lock Owner Info	Specify whether or not the user can change fields in the Owner options screen on the BlackBerry device. • **1**: Lock Information text • **2**: Lock Name text • **3**: Lock both Name and Information text	–	Java based or C++-based	4.0 (Java based BlackBerry device) or 2.7 (C++-based BlackBerry device)	4.0	–	Use this IT policy rule to lock the text defined in the Set Owner Info and Set Owner Name rules. You can overwrite this information by sending the Set Owner Information IT Admin command to the BlackBerry device.
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Java based only	4.0	–	–	–

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Set Owner Info	Specify the owner information that is set on the BlackBerry device.	–	Java based or C++-based	4.0 (Java based BlackBerry device) or 2.7 (C++-based BlackBerry device)	4.0	4.0	Use the Lock Owner Info rule to prevent the user from editing the owner information. **Warning**: The owner information is overwritten by the Set Owner Information IT Admin command.
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Java based only	4.0	–	–	–
Set Owner Name	Specify the owner name that is set on the BlackBerry device.	–	Java based or C++-based	4.0 (Java based BlackBerry device) or 2.7 (C++-based BlackBerry device)	4.0	4.0	Use the Lock Owner Info rule to prevent the user from editing the owner name. **Warning:** The owner name is overwritten by the Set Owner Information IT Admin command.
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Java based only	4.0	–	–	–

Desktop policy group

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Desktop Allow Desktop Add-ins	Specify whether or not the BlackBerry Desktop Software enables the user to set and run desktop add-ins (third-party COM-based extensions that access the BlackBerry device databases during synchronization).	True	Java based or C++-based	– BlackBerry Desktop Software version 3.6.1	4.0	–	–
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	3.6	–	–

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported				
Desktop Allow Device Switch	Specify whether or not the BlackBerry Desktop Software allows users to switch BlackBerry devices.	True	Java based or C++-based	– BlackBerry Desktop Manager version 3.6.1	4.0	–	Set this IT policy rule to False to prevent users from switching to use other BlackBerry devices.
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	3.6.1	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported				
Desktop Password Cache Timeout	Specify the length of time, in minutes, that the desktop caches the BlackBerry device password in memory.	10	Java based or C++-based	– BlackBerry Desktop Manager version 3.6	4.0	–	**Rule dependency**: The BlackBerry device uses this IT policy rule only if the Password Required rule is set to True. If you set this IT policy rule to 0, the BlackBerry device clears the password cache only when the BlackBerry device physical connection to the desktop computer is terminated, regardless of the length of time it is connected.
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	3.6	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported				

Desktop-Only items

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Auto Backup Enabled	Specify whether or not the option to back up the BlackBerry device is enabled automatically.	False	–	– BlackBerry Desktop Manager version 3.5	4.0	–	Set this IT policy rule to True to permit BlackBerry Desktop Manager to update the status in the backup and restore settings, and to enable clean recovery of the BlackBerry device data in the event that the BlackBerry device must be replaced.
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	3.5	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported				
Auto Backup Exclude Messages	Specify whether or not messages are excluded from automatic backups.	False	–	– BlackBerry Desktop Manager version 3.5	4.0	–	**Rule dependency**: If you set this IT policy rule to True, you must set the Auto Backup Include All rule to False.
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	3.5	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported				
Auto Backup Exclude Sync	Specify whether or not synchronized application data (data configured for synchronization) is excluded from automatic backups.	False	–	– BlackBerry Desktop Manager version 3.5	4.0	–	**Rule dependency**: If you set this IT policy rule to True, you must set the Auto Backup Include All rule to False.
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	3.5	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported				

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Auto Backup Frequency	Specify the frequency of automatic BlackBerry device data backups, in days.	7	—	— BlackBerry Desktop Manager version 3.5	4.0	—	Set this value to 2 or more days so that changes can be made on the BlackBerry device to data that is stored between backups. Save backup files to a network drive if the user's local hard disk space is limited.
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			—	—	3.5	—	—
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported				
Auto Backup Include All	Specify whether or not all data is included in automatic backups.	True	—	— BlackBerry Desktop Manager version 3.5	4.0	—	If you set this IT policy rule to True, the Backup all BlackBerry device application data option in the Backup and Restore options of the BlackBerry Desktop Manager is selected. Set this IT policy rule to False if you set the Auto Backup Exclude Sync and Auto Backup Exclude Messages rules to True.
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			—	—	3.5	—	—
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported				
Disable Wireless Calendar	Specify whether or not the wireless calendar synchronization option (BlackBerry Wireless Sync) is available to users in the calendar option.	False	—	— BlackBerry Desktop Manager version 3.5	4.0	—	Set this IT policy rule to False to enable the wireless calendar synchronization feature.
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			—	—	3.5	—	—
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported				

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Do Not Save Sent Messages	Specify whether or not the BlackBerry device saves a copy of each message that the user sends in a Sent messages folder.	—	—	— BlackBerry Desktop Manager version 3.5	4.0	—	Set this IT policy rule to False so that the messaging server stores messages sent from the BlackBerry device.
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			—	—	3.5	—	—
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported				
Force Load Count	Specify the number of times users can decline to update their BlackBerry devices before the update is forced.	No limit	—	— BlackBerry Desktop Manager version 3.5	4.0	—	To turn off the forced update functionality, set this IT policy rule to -1.
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			—	—	3.5	—	—
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported				
Force Load Message	Specify the message that appears when users are prompted to update to a later version of the device software.	—	—	— BlackBerry Desktop Manager version 3.5	4.0	—	**Rule dependency**: The BlackBerry device uses this IT policy rule only if you set the Force Load Count rule to a positive number.
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			—	—	3.5	—	—
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported				
Forward Messages In Cradle	Specify whether or not the BlackBerry device receives messages while it is connected to the computer using the cradle or a Universal Serial Bus (USB) cable.	The BlackBerry Enterprise Server sets this value.	—	— BlackBerry Desktop Manager version 3.5	4.0	—	When you set this IT policy rule, the BlackBerry Desktop Manager updates the status in the redirector settings.
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			—	—	3.5	—	—
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported				
Message Conflict Mailbox Wins	Specify whether or not the desktop mailbox wins when a conflict occurs between the desktop and the BlackBerry device during Personal Information Management (PIM) synchronization.	True	—	— BlackBerry Desktop Manager version 3.5	4.0	—	—
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			—	—	3.5	—	—

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported				
Message Prompt	Specify the message to appear when the BlackBerry Desktop Manager starts.	—	—	— BlackBerry Desktop Manager version 3.5	4.0	—	—
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			—	—	3.5	—	—
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported				
Show Application Loader	Specify whether or not the user has access to the application loader in the Desktop Software.	True	—	3.5	4.0	—	—
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			—	—	3.5	—	—
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported				
Show Web Link	Specify whether or not the user has access to the Web Link icon in the desktop software.	False	Java based or C++-based	— BlackBerry Desktop Manager version 3.5	4.0	—	The Web Link icon appears only if the default URL is set using the Web Link URL rule.
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			—	—	3.5	—	—
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported				
Sync Messages Instead Of Import	Specify whether or not the BlackBerry device permits message and folder synchronization instead of importing moves and deletions.	True	—	— BlackBerry Desktop Manager version 3.5	4.0	—	—
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			—	—	3.5	—	—
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported				
Web Link Label	Specify the label for the Web Link icon, if it appears. Setting this value does not imply that the Web Link icon is visible.	Downloads	—	— BlackBerry Desktop Manager version 3.5	4.0	—	Set the label according to your company requirements. **Rule dependency:** If you set this IT policy rule, you must also set the Show Web Link rule to True.
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			—	—	3.5	—	—
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported				

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Web Link URL	Specify the URL for the Web Link icon, if it appears. Setting this value does not imply that the Web Link icon is visible.	—	—	— BlackBerry Desktop Manager version 3.5	4.0	—	Set the URL according to your company requirements. **Rule dependency**: If you set this IT policy rule, you must also set the Show Web Link rule to True.
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			—	—	3.5	—	—
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported				

Device IOT Application policy group

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Device Diagnostic App Disable	Specify whether or not to prevent the user from accessing the Device Diagnostic Application on applicable BlackBerry devices.	False	Java based	4.2	4.0.6	–	–
Set Diagnostic Report Email Address	Type one ore more destination email addresses for the diagnostic report. Separate multiple email addresses by a comma.	False	Java based	4.2	4.0.6	–	–
Set Diagnostic Report PIN Address	Type one ore more destination PIN addresses for the diagnostic report. Separate multiple PIN addresses by a comma.	False	Java based	4.2	4.0.6	–	–

Device-Only items

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Allow BCC Recipients	Specify whether or not users can include blind carbon copy (BCC) recipients when composing email messages on the BlackBerry device.	True	Java based or C++-based	3.6 (Java based BlackBerry device) or 2.5 (C++-based BlackBerry device)	4.0	1.2 2.0 2.1 4.0	–
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	3.5	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Java based only	4.0	–	–	–

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Allow Peer-to-Peer Messages	Specify whether or not the users can send PIN messages from the BlackBerry device. **Note**: To block incoming PIN messages, set the Firewall Block Incoming Messages IT policy rule in the Security Policy Group.	True	Java based or C++-based)	3.6 (Java based BlackBerry device) or 2.5 (C++-based BlackBerry device)	4.0	1.2 2.0 2.1 4.0	Set this IT policy rule to False to hide the PIN messaging functionality on the BlackBerry device. **Warning**: Setting this IT policy rule to False does not prevent users from receiving PIN messages.
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	3.5	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Java based only	4.0	–	–	–
Allow SMS	Specify whether or not the BlackBerry device permits sending Short Message Service (SMS) messages (text messaging). **Note**: To block incoming text, or SMS, messages, set the Firewall Block Incoming Messages IT policy rule in the Security Policy Group.	True	Java based	3.6	4.0	1.2 2.0 2.1 4.0	Set this rule to False to hide text messaging functionality on the BlackBerry device.
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	3.5	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			–	4.0	–	–	–
Default Browser Config UID	Specify a unique ID for the Browser Config Service Record, which sets the default browser on the BlackBerry device (for example, when opening links in messages).	–	Java based	3.6	4.0	4.0 (internal) **Note**: The transport stack does not report this IT policy rule to the BlackBerry connect application.	–
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	3.5	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			–	4.0	–	–	–

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Enable Long-Term Timeout	Specify whether or not the BlackBerry device locks after a predefined period of time, regardless of user activity.	—	Java based	3.6	4.0	1.2 2.0 2.1 4.0	Set this IT policy rule to True to force the BlackBerry device to lock automatically after 60 minutes (the default period). Use the Periodic Challenge Time rule to shorten this interval.
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			—	—	3.5	—	—
BlackBerry Enterprise Server for Novell GroupWise exceptions:			—	4.0	—	—	—
Enable WAP Config	Specify whether or not the Wireless Application Protocol (WAP) Browser icon appears on the BlackBerry device when the service provider provisions the WAP browser with the appropriate service books present.	True	Java based	3.6	4.0	2.1 4.0	Set this IT policy rule to False to hide the WAP Browser icon on the BlackBerry device.
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			—	—	3.5	—	—
BlackBerry Enterprise Server for Novell GroupWise exceptions:			—	4.0	—	—	—
Home Page Address	Specify the URL address of the home page used by the browser on the BlackBerry device.	—	Java based or C++-based	3.6 (Java based BlackBerry device) or 2.5 (C++-based BlackBerry device)	4.0	4.0 (internal)	Most companies set the URL to their intranet address. If this IT policy rule is not set, the BlackBerry device uses the default home page URL.
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			—	—	3.5	—	—
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Java based only	4.0	—	—	—
Home Page Address is Read-Only	Specify if the user can modify the URL address of the browser home page.	—	Java based or C++-based	3.6 (Java based BlackBerry device) or 2.5 (C++-based BlackBerry device)	4.0	4.0 (internal)	—

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	3.5	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Java based only	4.0	–	–	–
Maximum Password Age	Specify the number of days from when users set a BlackBerry device password until the password expires and their BlackBerry device prompts the users to type a new password.	–	Java based or C++-based	3.6 (Java based BlackBerry device) or 2.5 (C++-based BlackBerry device)	4.0	1.2 2.0 2.1 4.0	**Rule dependency:** The BlackBerry device uses this IT policy rule only if the Password Required rule is set to True. Set this IT policy rule according to your company password expiration policy. If no such policy exists, RIM recommends setting a maximum password age of 30 days. If you set this rule to 0, password aging is turned off.
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	3.6	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Java based only	4.0	–	–	–

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Maximum Security Timeout	Specify the maximum time, in minutes, that a BlackBerry device user can set as the security timeout value (the number of minutes of BlackBerry device user inactivity allowed before the security timeout occurs and the BlackBerry device requires the user to type the BlackBerry device password to unlock the BlackBerry device). The BlackBerry device user can set any timeout value that is less than or equal to the maximum value unless you set the User Can Change Timeout rule value to False. The maximum security timeout value available by default on the BlackBerry device is 60 minutes. Use the Set Password Timeout rule to set a specific timeout value.	—	Java based	4.0	4.0	1.2 2.0 2.1 4.0	Set this IT policy rule according to your company security policy. If no such policy exists, RIM recommends setting a maximum timeout value of 30 minutes. **Rule dependency:** The BlackBerry device uses this IT policy rule only if the Password Required rule is set to True.

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Minimum Password Length	Specify the minimum allowable length, in characters, of the BlackBerry device security password.	The valid range is between 4 and 14 characters.	Java based or C++-based	3.6 (Java based BlackBerry device) or 2.5 (C++-based BlackBerry device)	4.0	1.2 2.0 2.1 4.0	Set this IT policy rule according to your company password length policy. If no such policy exists, RIM recommends setting a minimum length of 8 characters. **Rule dependency**: The BlackBerry device uses this IT policy rule only if the Password Required rule is set to True. **Warning**: If the FIPS Level rule is set to 2, the BlackBerry device enforces a minimum length of 5 characters by default.
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	3.5	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Java based only	4.0	–	–	–

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Password Pattern Checks	Specify whether or not to verify that the BlackBerry device security password matches certain character pattern requirements. • **0**: no restriction • **1**: requires at least 1 alpha and 1 numeric character • **2**: requires at least 1 alpha, 1 numeric and 1 special character • **3**: requires at least 1 uppercase alpha, 1 lowercase alpha, 1 numeric and 1 special character	0	Java based or C++-based	3.6 (Java based BlackBerry device) or 2.5 (C++-based BlackBerry device)	4.0	1.2 2.0 2.1 4.0	**Note**: By default, the BlackBerry device prevents setting passwords that use a natural sequence of characters or numbers (in other words, consecutively listed or consistently offset) by default. If a symbol is inserted into an otherwise naturally sequenced password string, the BlackBerry device allows the password. To enable a higher level of security, RIM recommends setting this value to a minimum of 1. **Warning**: If options 2 or 3 are selected, password pattern checking is unavailable on C++-based BlackBerry devices.
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	3.5	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Java based only	4.0	–	–	–
Password Required	Specify whether or not the user must set and use a password to use to authenticate to the BlackBerry device.	False; a password is not required on the BlackBerry device.	Java based or C++-based	3.6 (Java based BlackBerry device) or 2.5 (C++-based BlackBerry device)	4.0	1.2 2.0 2.1 4.0	**Warning**: If the FIPS Level rule is set to 2, the BlackBerry device requires the user to set a password by default.

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	3.5	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Java based only	4.0	–	–	–
User Can Change Timeout	Specify whether or not the BlackBerry device user can override the security timeout value (if you set it) and set a value in the allowed range on the BlackBerry device.	True	Java based	3.6	4.0	1.2 2.0 2.1 4.0	Set this IT policy rule according to your company security policy. If no such policy exists, RIM recommends setting the Set Security Timeout rule and then setting the User Can Change Timeout rule to False.
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	3.5	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			–	4.0	–	–	–
User Can Disable Password	Specify whether or not the user can turn off the password requirement.	True	Java based or C++-based	3.6 (Java based BlackBerry device) or 2.5 (C++-based BlackBerry device)	3.5	1.2 2.0 2.1 4.0	Set this IT policy rule to **False** to prevent users from turning off the password on the BlackBerry device. **Rule dependency**: The BlackBerry device uses this IT policy rule only if the Password Required rule is set to True. **Warning**: This IT policy rule is obsolete in BlackBerry device software versions 4.0 (Java based BlackBerry devices) and 2.7 (C++-based BlackBerry devices).

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Java based only	4.0	4.0	–	–

Global items

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Allow Browser	Specify whether or not the BlackBerry device permits the user to use the default browser included on the BlackBerry device.	True	Java based or C++-based	3.6 (Java based BlackBerry device) or 2.5 (C++-based BlackBerry device)	4.0	1.2 2.0 2.1 4.0 (internal)	–
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	3.5	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Java based only	4.0	–	–	–
Allow Phone	Specify whether or not the phone functionality on the BlackBerry device is available to the user.	True	Java based	3.6	4.0	1.2 2.0 2.1 4.0	Set this IT policy rule to False to prevent users from making any phone calls except emergency calls. The phone icon is still visible to users.
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	3.5	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			–	4.0	–	–	–
Auto Signature	Specify the signature that is attached automatically to the user's messages.	–	–	– BlackBerry Desktop Manager version 3.5	4.0	–	Use this IT policy rule to add a disclaimer to the end of outgoing messages sent from the BlackBerry device.
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	3.5	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported	Not supported	Not supported	–	–

MDS policy group

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Disable activation with public MDSS	Specify whether or not the BlackBerry device can connect to public BlackBerry MDS Services.	False	Java based	4.2	4.1.2	–	–
Disable user-initiated activation with MDSS	Specify whether or not the BlackBerry device user can initiate a connection with BlackBerry MDS Services.	False	Java based	4.2	4.1.2	–	Set this IT policy rule to True to prevent the user from initiating the BlackBerry MDS Services connection.
Disable MDS Runtime Environment	Specify whether or not the BlackBerry Mobile Data System (MDS) Runtime™ environment is disabled on the BlackBerry device.	False	Java based	4.0	4.1.0	–	Set this IT policy rule to True to prevent the user from activating the BlackBerry MDS Runtime environment.

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Lowest security version allowed	Specify the lowest security version permitted for the BlackBerry Mobile Data System: 1 = Permits BlackBerry devices running BlackBerry MDS Runtime Environment versions 1.1.0 or later to communicate with all versions of BlackBerry MDS Services. 2 = Permits BlackBerry devices running BlackBerry MDS Runtime Environment versions 1.1.0 or later to communicate with BlackBerry MDS Services versions 4.1.2 or later only. The security version affects the compatibility of versions of BlackBerry MDS Runtime Environment versions 1.1.0 and later and BlackBerry MDS Services.	1	Java based	4.2	4.1.2	—	—
Verify MDSS certificate	Specify whether or not the BlackBerry MDS Runtime Environment version 1.1.0 or later verifies the BlackBerry Mobile Data System (MDS) Service certificate.	True	Java based	4.2	4.1.2	—	If you set this IT policy rule to False, BlackBerry MDS Services permits unauthenticated connections. from BlackBerry devices running BlackBerry MDS Runtime Environment version 1.1.0 or later.

Memory Cleaner policy group

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Force Memory Clean When Holstered	Specify whether or not the BlackBerry device performs a memory clean while it is holstered.	False	Java based	3.6	– S/MIME Support Package version 1.5	4.0	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported	Not supported	Not supported	–	–
Force Memory Clean When Idle	Specify whether or not the BlackBerry device performs a memory clean while it is idle.	False	Java based	3.6	– S/MIME Support Package version 1.5	4.0	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported	Not supported	Not supported	–	–
Memory Cleaner Maximum Idle Time	Specify the maximum idle time, in minutes, that elapses before the memory cleaner starts.	1	Java based	3.6	– S/MIME Support Package version 1.5	4.0	**Rule dependency**: The BlackBerry device uses this IT policy rule only if you set the Force Memory Clean When Idle rule to True.
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported	Not supported	Not supported	–	–

On-Device help policy group

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
On-Device Help Links	Specify Uniform Resource Indicators (URIs) or links to add to the On-Device Help index page using the format "uri1|label1|...|uri*N*|label*N*".	–	Java based	4.1	4.0.3	–	If you specify multiple links, you should also set the On-Device Help Group Label IT policy rule.

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
On-Device Help Group Label	Specify a label to use for multiple on-device help links.	—	Java based	4.1	4.0.3	—	Set an on-device help group label if you specify multiple links using the On-Device Help Links rule.

Password policy group

The BlackBerry device uses the following rules only if you set the Password Required rule to True.

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Duress Notification Address	Specify the message account address that receives notification when users type their BlackBerry device security passwords under duress (in other words, users indicate that they are unlocking their BlackBerry devices against their will). The user can indicate duress by moving the first character to the end of the password when typing. For example, if the BlackBerry device password is blackberry, the duress password is lackberryb. **Warning**: If you set this IT policy rule, the set maximum number of password attempts is effectively reduced by half; each time the user types a password to unlock the BlackBerry device, the BlackBerry device must confirm whether the password attempt is either the correct password or the correct duress password.	–	Java based	4.0	4.0	4.0	This IT policy rule enables users to notify administrators if the BlackBerry device is in danger of being stolen. If no address is specified, the duress password function is not activated. **Warning**: To prevent a party who has stolen the unlocked BlackBerry device from receiving a response to the duress notification on the BlackBerry device, the message account you specify to receive duress notification messages should be active and not have an out of office or other auto-reply function set.

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Forbidden Passwords	Specify the password(s) that users are not permitted to use.	–	Java based	4.1	4.0.2	–	To compose a list of forbidden passwords, use commas to separate passwords. **Note**: By default, the BlackBerry device prevents setting passwords that use a natural sequence of characters or numbers (in other words, consecutively listed or consistently offset) by default. If a symbol is inserted into an otherwise naturally sequenced password string, the BlackBerry device allows the password.
Maximum Password History	Specify the maximum number of previous passwords against which new passwords are checked to prevent re-use of old passwords.	0	Java based	3.6	4.0	1.2 2.0 2.1 4.0	If this IT policy rule is set to 0, password checking is turned off.
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	3.6	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			–	4.0	–	–	–

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Periodic Challenge Time	Specify the interval, in minutes, after which the BlackBerry device prompts the user to type a password, regardless of whether the BlackBerry device has been idle or in use during that interval.	60	Java based	4.0	4.0	4.0	Set this IT policy rule according to your company security policy. If no such security policy exists, enforce this IT policy rule by setting the Enable Long-Term Timeout policy rule. Setting this IT policy rule restricts the timeout settings available on the BlackBerry device. You can also set the User Can Change Timeout policy rule to False.
Set Maximum Password Attempts	Specify the number of security password attempts (incorrect passwords entered) that the BlackBerry device permits before it erases all of its data and becomes unavailable.	10	Java based	3.6	4.0	1.2 2.0 2.1 4.0	The maximum number of password attempts is set to 10 by default on the BlackBerry device. Use this IT policy rule to lower the number of password attempts.
BlackBerry Enterprise Server for Novell GroupWise exceptions:			—	4.0	—	—	—

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Set Password Timeout	Specify the number of minutes of BlackBerry device user inactivity allowed before the security timeout occurs and the BlackBerry device requires the user to type the BlackBerry device password to unlock the BlackBerry device.	2 minutes	Java based	3.6	4.0	1.2 2.0 2.1 4.0	Use this IT policy rule to change the default security timeout interval. **Rule dependencies:** The BlackBerry device uses this IT policy rule only if the Password Required rule is set to True. If you do not set the User Can Change Timeout rule to False, the BlackBerry device user can set the password timeout to one of a range of values.
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	3.6	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			–	4.0	–	–	–
Suppress Password Echo	Specify whether or not echoing (printing to the screen) characters typed into the Security password screen after a given number of failed attempts to unlock the BlackBerry device is turned on.	True	Java based	3.6	4.0	1.2 2.0 2.1 4.0	Password echo is turned on by default on the BlackBerry device. Use this IT policy rule to override the default. **Warning:** If the FIPS Level rule is set to 2, the BlackBerry device suppresses password echoing by default.
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	3.6	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			–	4.0	–	–	–

PIM Sync policy group

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Disable Address Wireless Sync	Specify whether or not wireless address database synchronization is turned off.	False	Java based or C++-based	4.0 (Java based BlackBerry device) or 2.7 (C++-based BlackBerry device)	4.0	4.0 (internal)	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Java based only	4.0	–	–	–
Disable All Wireless Sync	Specify whether or not wireless synchronization of all personal information management (PIM) databases is turned off.	False	Java based or C++-based	4.0 (Java based BlackBerry device) or 2.7 (C++-based BlackBerry device)	4.0	4.0 (internal)	Set this IT policy rule to True to turn off synchronization of contacts, memos, tasks, and calendar. **Note**: This IT policy rule does not change wireless message reconciliation. Users can still send and receive messages.
Disable Calendar Wireless Sync	Specify whether or not wireless synchronization of the calendar database is turned off.	False	Java based or C++-based	4.0 (Java based BlackBerry device) or 2.7 (C++-based BlackBerry device)	4.0	4.0 (internal)	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Java based only	4.0	–	–	–

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Disable Enterprise Activation Progress	Specify whether or not the BlackBerry device Home screen displays Enterprise Activation progress.	True	Java based	4.2	4.0.6	–	If you set this IT policy rule to True, the BlackBerry device hides the Enterprise Activation icon and progress status on the Home screen.
Disable Memopad Wireless Sync	Specify whether or not wireless synchronization of the memo pad database is turned off.	False	Java based or C++-based	4.0 (Java based BlackBerry device) or 2.7 (C++-based BlackBerry device)	4.0	4.0 (internal)	–
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	–	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Java based only	4.0	–	–	–
Disable Phone Call Log Wireless Sync	Specify whether or not wireless synchronization of the phone call log database is turned off.	False	Java based only	4.1	4.1	–	–
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	–	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			–	4.0	–	–	–
Disable PIN Messages Wireless Sync	Specify whether or not wireless synchronization of the PIN messages database is turned off.	True	Java based only	4.1	4.1	–	**Warning:** If you set this IT policy rule to False, the BlackBerry Enterprise Server logs all PIN messages in unencrypted format to the specified log file. Make sure that the log file is in a location for which your corporate security policies restrict internal and external user access.
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	–	–	–

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
BlackBerry Enterprise Server for Novell GroupWise exceptions:			–	4.0	–	–	–
Disable SMS Messages Wireless Sync	Specify whether or not wireless synchronization of the SMS messages database is turned off.	True	Java based only	4.1	4.1	–	**Warning:** If you set this IT policy rule to False, the BlackBerry Enterprise Server logs all SMS messages in unencrypted format to the specified log file. Make sure that the log file is in a location for which your corporate security policies restrict internal and external user access.
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	–	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			–	4.0	–	–	–
Disable Task Wireless Sync	Specify whether or not wireless synchronization of the task database is turned off.	False	Java based or C++-based	4.0 (Java based BlackBerry device) or 2.7 (C++-based BlackBerry device)	4.0	4.0 (internal)	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Java based only	4.0	–	–	–

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Disable Wireless Bulk Loads	Specify whether or not wireless synchronization of PIM data during enterprise activation or as part of a backup and restore operation is turned off.	False	Java based or C++-based	4.0 (Java based BlackBerry device) or 2.7 (C++-based BlackBerry device)	4.0	4.0 (internal)	Set this IT policy rule to True to minimize wireless data transfers when activating or updating BlackBerry devices. The BlackBerry device must be physically connected to a computer before the data transfer starts. **Note**: If the BlackBerry device is disconnected from the desktop computer during a bulk load, the BlackBerry Desktop Software sends the remainder of the data over the wireless network.
BlackBerry Enterprise Server for Novell GroupWise exceptions:			—	4.0	—	—	—

PGP Application policy group

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
PGP Allowed Content Ciphers	Specify the content ciphers that the BlackBerry device can use to send encrypted PGP® messages. • **0**: AES (256-bit) • **1**: AES (192-bit) • **2**: AES (128-bit) • **3**: CAST (128-bit) • **5**: Triple DES	Allow all content ciphers	Java based	4.1 PGP Support Package version 4.1	4.0.2	–	**Warnings**: To maintain compatibility with most PGP clients, enable Triple DES and, or CAST. The BlackBerry device encrypts the message using Triple DES by default if it does not know the decryption capabilities of the recipient. If the FIPS Level rule is set to 2, the BlackBerry device uses AES (256-bit), AES (192-bit), AES (128-bit), and Triple DES.
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported	Not supported	Not supported	–	–
PGP Blind Copy Address	Specify an address that is added as a BCC recipient to all outgoing encrypted PGP messages.	–	Java based	4.1 PGP Support Package version 4.1	4.0.2	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported	Not supported	Not supported	–	–
PGP Force Digital Signature	Specify whether or not all outgoing PGP messages are digitally signed. **Warning**: If you apply this IT policy rule, you might overrule secure email policy settings on the PGP Universal Server.	False	Java based	4.1 PGP Support Package version 4.1	4.0.2	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported	Not supported	Not supported	–	–

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
PGP Force Encrypted Messages	Specify whether or not all outgoing PGP messages are encrypted. **Warning**: If you apply this IT policy rule, you might overrule secure email policy settings on the PGP Universal Server.	False	Java based	4.1 PGP Support Package version 4.1	4.0.2	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported	Not supported	Not supported	–	–
PGP Minimum Strong DH Key Length	Specify the minimum DH key size, in bits, that the BlackBerry device allows for use in the PGP application.	1024	Java based	4.1 PGP Support Package version 4.1	4.0.2	–	Set the Disable Weak Certificate Use rule to True to prevent users from sending messages using certificates that have weak corresponding public keys.
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported	Not supported	Not supported	–	–
PGP Minimum Strong DSA Key Length	Specify the minimum DSA key size, in bits, allowed for use in the PGP application.	1024	Java based	4.1 PGP Support Package version 4.1	4.0.2	–	Set the Disable Weak Certificate Use rule to True to prevent users from sending messages using certificates that have weak corresponding public keys.
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported	Not supported	Not supported	–	–
PGP Minimum Strong RSA Key Length	Specify the minimum RSA key size, in bits, allowed for use in the PGP application.	1024	Java based	4.1 PGP Support Package version 4.1	4.0.2	–	Set the Disable Weak Certificate Use rule to True to prevent users from sending messages using certificates that have weak corresponding public keys.
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported	Not supported	Not supported	–	–

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
PGP Universal Enrollment Method	Specify the method users must use to enroll with the PGP Universal Server from their BlackBerry devices. • **0**: The BlackBerry device prompts users to type their domain user name and password. • **1**: The BlackBerry device prompts users to type their email address.	1 (prompt for email address)	Java based	4.1 PGP Support Package version 4.1	4.0.2	—	Users must type and submit their enrollment (user name or email address) information before sending and receiving PGP messages on their BlackBerry devices.
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported	Not supported	Not supported	—	—
PGP Universal Policy Cache Timeout	Specify the length of time, in hours, that the BlackBerry device caches the PGP Universal Server address.	24	Java based	4.1 PGP Support Package version 4.1	4.0.2	—	—
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported	Not supported	Not supported	—	—
PGP Universal Server Address	Specify the address of the company's PGP Universal Server.	—	Java based	4.1 PGP Support Package version 4.1	4.0.2	—	—
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported	Not supported	Not supported	—	—

S/MIME Application policy group

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Entrust Messaging Server (EMS) Email Address	Specify the email address for your company Entrust® Entelligence™ Messaging Server. Leave empty if your company does not use an Entrust Entelligence Messaging Server.	–	Java based	4.0	– S/MIME Support Package version 4.0	4.0	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported	Not supported	Not supported	–	–
S/MIME Allowed Content Ciphers	Specify the content ciphers used to send S/MIME messages: • **0**: AES (256-bit) • **1**: AES (192-bit) • **2**: AES (128-bit) • **3**: CAST (128-bit) • **4**: RC2 (128-bit) • **5**: Triple DES • **6**: RC2 (64-bit) • **7**: RC2 (40-bit)	Allow all content ciphers	Java based	3.6 S/MIME Support Package version 1.5	3.6	4.0	**Warnings**: To maintain compatibility with most S/MIME clients, enable Triple DES and, or one of the RC2 ciphers. The BlackBerry device encrypts the message using Triple DES by default if it does not know the decryption capabilities of the recipient. If the FIPS Level rule is set to 2, the BlackBerry device uses AES (256-bit), AES (192-bit), AES (128-bit), and Triple DES.
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported	Not supported	Not supported	–	–
S/MIME Blind Copy Address	Specify an address that is added as a BCC recipient to all outgoing S/MIME messages.	–	Java based	3.6 S/MIME Support Package version 1.5	3.6	4.0	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported	Not supported	Not supported	–	–

Policy rule	Description	Default setting	Minimum requirements				Use	
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack		
S/MIME Force Digital Signature	Specify whether or not all outgoing S/MIME messages are signed digitally.	False	Java based	3.6 S/MIME Support Package version 1.5	3.6	4.0		–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported	Not supported	Not supported		–	–
S/MIME Force Encrypted Messages	Specify whether or not all outgoing S/MIME messages are encrypted.	False	Java based	3.6 S/MIME Support Package version 1.5	3.6	4.0		–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported	Not supported	Not supported		–	–
S/MIME Force Smartcard Use	Specify whether or not all key operations must be performed using an attached BlackBerry Smart Card Reader.	False	Java based	3.6 S/MIME Support Package version 1.5	3.6	4.0		–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported	Not supported	Not supported		–	–
S/MIME Minimum Strong DH Key Length	Specify the minimum DH key size, in bits, that the BlackBerry device allows for use in the S/MIME application.	1024	Java based	3.6 S/MIME Support Package version 1.5	3.6	4.0		–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported	Not supported	Not supported		–	–
S/MIME Minimum Strong DSA Key Length	Specify the minimum DSA key size, in bits, that the BlackBerry device allows for use in the S/MIME application.	1024	Java based	3.6 S/MIME Support Package version 1.5	3.6	4.0		–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported	Not supported	Not supported		–	–
S/MIME Minimum Strong ECC Key Length	Specify the minimum ECC key size, in bits, that the BlackBerry device allows for use in the S/MIME application.	163	Java based	3.6 S/MIME Support Package version 1.5	3.6	4.0		–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported	Not supported	Not supported		–	–

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
S/MIME Minimum Strong RSA Key Length	Specify the minimum RSA key size, in bits, allowed for use in the S/MIME application.	1024	Java based	3.6 S/MIME Support Package version 1.5	3.6	4.0	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported	Not supported	Not supported	–	–

Secure Email policy group

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Canonical Certificate Domain Name	Specify the domain name used for the email addresses contained in certificates issued within your organization.	False	Java based	4.2	4.0.6	–	Consider setting this IT policy rule if your organization's users certificates contain a long-lived email address but the users typically send email messages from a shorter-lived email address with the same username component and a different domain component. **Note**: The BlackBerry device uses both the short-lived and long-lived email address when searching for certificates for use with secure email.

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Disable Certificate Address Checks	Specify whether or not the BlackBerry device displays a warning when the user receives a signed message on the BlackBerry device in which the sender's email address does not appear in the certificate or PGP key used to sign the message.	False	Java based	4.2	4.0.6	–	Consider setting this IT policy rule to True if your organization's user certificates contain email addresses that are different from the addresses that the users typically use to send email.

Security policy group

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Allow External Connections	Specify whether or not applications, including third-party applications, on the BlackBerry device can initiate external connections (for example, to WAP, SMS, or other public gateways).	True	Java based	3.6	4.0	4.0 (internal)	–
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	3.6	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			–	4.0	–	–	–
Allow Internal Connections	Specify whether or not applications, including third-party applications, on the BlackBerry device can initiate internal connections (for example, to the BlackBerry MDS Connection Service.	True	Java based	3.6	4.0	4.0 (internal)	–
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	3.6	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			–	4.0	–	–	–
Allow Outgoing Call When Locked	Specify whether or not users can place calls when the BlackBerry device is security -locked.	False	Java based	4.0	4.0	4.0	–

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Allow Smart Card Password Caching	Specify whether or not the BlackBerry device can cache the smart card password.	False	Java based	4.0	4.0	4.0	Set this IT policy rule to True to enable the BlackBerry device to cache the smart card password for a period of time controlled by the key store private key timeout. The memory cleaner clears the cached passwords.
Allow Split-Pipe Connections	Specify whether or not applications, including third-party applications, can open internal and external connections simultaneously on the BlackBerry device.	False	Java based	3.6	4.0	4.0	Enabling split-pipe connections presents a security issue because, when enabled, applications can collect data from inside the firewall and send it outside the firewall without any auditing.
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	3.6	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			–	4.0	–	–	–
Allow Third Party Apps to Use Persistent Store	Specify whether or not third-party applications can use the RIM persistent store application programming interface (API).	True	Java based	3.6	3.6	–	This IT policy rule is made obsolete by BlackBerry Enterprise Server for Microsoft Exchange version 3.6.2
Allow Third Party Apps to Use Serial Port	Specify whether or not third-party applications can use the serial port, Infrared Data Association (IrDA), or USB ports on the BlackBerry device.	True	Java based	3.6	4.0	4.0	–
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	3.6	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			–	4.0	–	–	–

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Certificate Status Maximum Expiry Time	Specify the maximum length of time, in hours, that a certificate status can remain on the BlackBerry device before it should be updated in the certificate synchronization manager and the BlackBerry device key store.	4	Java based	4.0	4.0	4.0	–
Content Protection Strength	Specify whether or not content protection is turned on by selecting the cryptography strength that the BlackBerry device uses to encrypt content that it receives while it is locked. • **Strong**: 160-bit ECC public key; provides good security and good performance, adequate for most situations • **Stronger**: 283-bit ECC public key; provides better security but slower performance than the Strong setting • **Strongest**: 571-bit ECC public key; provides the highest level of security but the slowest performance of the three settings	–	Java based	4.0	4.0	4.0	**Rule dependency**: If you set this IT policy rule to Strong or Stronger RIM recommends that you set the Minimum Password Length IT policy rule to 12 characters. If you set the content protection strength to Strongest RIM recommends that you also request that the user set a password of at least 21 characters. These password lengths maximize the encryption strength that the longer ECC keys are designed to provide. The BlackBerry device uses this IT policy rule only if the Password Required rule is set to True.

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Desktop Backup	Specify which BlackBerry device databases are backed up by a desktop. • **0**: All BlackBerry device databases • **1**: Minimal subset of BlackBerry device databases; generally, databases that some desktop components require access to for correct operation, such as certificate synchronization manager • **2**: No BlackBerry device databases	0	Java based	4.0	4.0	4.0	—
Disable 3DES Transport Crypto	Specify whether or not the BlackBerry device can use the Triple DES algorithm to encrypt and decrypt packets that the BlackBerry device and the BlackBerry Enterprise Server that sends the IT policy send between them.	False (The BlackBerry device and the BlackBerry Enterprise Server can use the Triple DES algorithm and the AES algorithm to encrypt and decrypt the packets that they send between them..)	Java based	4.0	4.0	4.0 (internal)	Set this IT policy rule to True to require the BlackBerry device and the BlackBerry Enterprise Server to use the AES algorithm to encrypt and decrypt the communication between them.
Disable Cut/ Copy/Paste	Specify whether or not the user can use the clipboard's cut, copy, and paste features on the BlackBerry device.	False	Java based	4.0	4.0	4.0	—
Disable External Memory	Specify whether or not the expandable memory (microSD) feature works on applicable BlackBerry devices.	False	Java based	4.2	4.0.6	—	—

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Disable Forwarding Between Services	Specify whether or not the user can forward or reply to a message on the BlackBerry device using a different BlackBerry Enterprise Server from the one that delivered the original message.	False	Java based	4.0	4.0	4.0	This IT policy rule also prevents forwarding or replying to a PIN message with a message account address and replying to an email message with a PIN message.
Disable Invalid Certificate Use	Specify whether or not the user can send a message from the BlackBerry device using an expired or unvalidated certificate.	False	Java based	3.6	4.0	4.0	If you set this IT policy rule to False, the BlackBerry device warns the user about but does not prevent the user from using an expired or unvalidated certificate.
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	3.6	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			–	4.0	–	–	–
Disable IP Modem	Specify whether or not the Internet Protocol (IP) modem feature on applicable BlackBerry devices is turned off.	False	Java based	4.0	4.0	4.0	Currently, this IT policy rule applies to the BlackBerry 7290 Wireless Handheld™ and BlackBerry 7100 Series.
Disable Key Store Backup	Specify whether or not the user can back up certificates and private keys in the BlackBerry device key stores.	False	Java based	4.0	4.0	4.0	–

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Disable Key Store Low Security	Specify whether or not the user can set the key store security level to low on the BlackBerry device.	False	Java based	3.6	4.0	4.0	Set this IT policy rule to True to automatically require the next highest key store level. For BlackBerry devices running BlackBerry Device Software version 3.6 the next security level is high. For BlackBerry devices running BlackBerry Device Software version 4.0 or later, the next security level is medium.
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	3.6	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			–	4.0	–	–	–
Disable Media Manager	Specify whether or not the user can access the Media Manager from the BlackBerry Desktop Software.	False	Java based	4.2	4.0.6	–	Set this IT policy rule to True to permit the user to access an external file system.
Disable Message Normal Send	Specify whether or not the BlackBerry device can send unencrypted email messages.	False	Java based	3.6	4.0	4.0	If you set this IT policy rule to True, to send email messages the S/MIME Support Package or the PGP Support Package must be installed on the BlackBerry device and enabled on the BlackBerry Enterprise Server.
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	3.6	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			–	4.0	–	–	–

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Disable Peer-to-Peer Normal Send	Specify whether or not the user can send plain text PIN messages when using the S/MIME Support Package or the PGP Support Package on the BlackBerry device.	False	Java based	3.6	4.0	4.0	If you set this IT policy rule to True, to send PIN messages the S/MIME Support Package or the PGP Support Package must be installed on the BlackBerry device and enabled on the BlackBerry Enterprise Server. To turn off all PIN messaging, set the Allow Peer-to-Peer Messages rule to False.
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			—	—	3.6	—	—
BlackBerry Enterprise Server for Novell GroupWise exceptions:			—	4.0	—	—	—
Disable Persisted Plain Text	Specify whether or not any application can persist the plain text form of a content-protected object in the persistent store (for example, the file system). If you set this IT policy rule to True, the BlackBerry device writes information about the application in the BlackBerry device Event Log and then resets, which returns the BlackBerry device to a valid known state.	False	Java based	4.0	4.0	4.0	**Warning**: Not all applications on the BlackBerry device work if you set this IT policy rule set to True. RIM recommends setting this IT policy rule only if you need assurance that sensitive data cannot persist in plain text form.

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Disable Radio When Cradled	Specify whether or not the radio is turned off when the BlackBerry device is connected to USB peripherals. • **0**: radio is not turned off when connected • **1**: radio is turned off when a USB cable is connected • **2**: radio is turned off when the connected USB peripheral enumerates	0	Java based	4.0	4.0	4.0	Only USB-enabled BlackBerry devices support this IT policy rule. Enumeration is the first part of the USB protocol. Before a USB peripheral can communicate with the BlackBerry device, it must enumerate. If you set this IT policy rule to 2, the radio turns off only when the BlackBerry device is connected to a USB device that needs to communicate with the BlackBerry device (for example a USB charger).
Disable Revoked Certificate Use	Specify whether or not outgoing messages are encrypted with revoked certificates.	False	Java based	3.6	4.0	4.0	If you set this IT policy rule to False, the BlackBerry device warns the user about but does not prevent the user from using a revoked certificate.
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			—	—	3.6	—	—
BlackBerry Enterprise Server for Novell GroupWise exceptions:			—	4.0	—	—	—

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Disable Smart Password Entry	Specify whether or not to disable the BlackBerry device option for the user to turn on smart password entry when using two factor authentication.	False	Java based	4.2	4.0.6	–	If you set the IT policy rule to True, the BlackBerry device resets any knowledge of the user's numeric passwords if the user is currently using smart password entry.
Disable Stale Certificate Status Checks	Specify whether or not the BlackBerry device should display warnings and visual indications if the user receives an email message that includes a certificate with stale status.	False	Java based	4.2	4.0.6	–	If you set this IT policy rule to True, the BlackBerry device does not display warnings and visual indications of stale certificate status. Consider setting this IT policy rule to True if your organization uses a PKI that does not update the status of certificates. **Rule dependency**: If you set this rule to True, the BlackBerry device ignores the Certificate Status Maximum Expiry Time rule setting and the status of certificates on the BlackBerry device never expires.
Disable Stale Status Use	Specify whether or not users can encrypt messages using a certificate with a stale status.	False	Java based	4.0	4.0	4.0	If you set this IT policy rule to False, the BlackBerry device warns the user about but does not prevent the user from using a stale certificate.

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Disable Untrusted Certificate Use	Specify whether or not users can send messages that are encrypted with a certificate that the BlackBerry device does not trust.	False	Java based	3.6	4.0	4.0	If you set this IT policy rule to False, the BlackBerry device warns the user about but does not prevent the user from using an untrusted certificate.
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	3.6	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			–	4.0	–	–	–
Disable Unverified Certificate Use	Specify whether or not users can send messages that are encrypted with a certificate that the BlackBerry device cannot verify.	False	Java based	4.0	4.0	4.0	If you set this IT policy rule to False, the BlackBerry device warns the user about but does not prevent the user from using an unverified certificate.
Disable Unverified CRLs	Specify whether or not users can accept unverified CRLs on the Mobile Data Service when checking the status of a certificate BlackBerry device.	False	Java based	4.0	4.0	–	–
Disable USB Mass Storage	Specify whether or not to disable the USB Mass Storage feature on applicable BlackBerry devices.	False	Java based	4.2	4.0.6	–	If you set this IT policy rule to True, the BlackBerry device cannot use an external file system connected to the USB port.

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Disable Weak Certificate Use	Specify whether or not users can send a message using a certificate that has a weak corresponding public key.	False	Java based	3.6	4.0	–	If you set this IT policy rule to False, the BlackBerry device warns the user about but does not prevent the user from using a certificate that has a weak corresponding public key. **Note**: Use the IT policy rules provided for each security application: • Transport Layer Security (TLS) • Wireless Transport Layer Security (WTLS) • S/MIME • PGP Set the minimum strength for each type of algorithm key length: • RSA • DSA • DH • ECC
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	3.6	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			–	4.0	–	–	–

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Disallow Third Party Application Downloads	Specify whether or not applications that are not digitally signed by RIM are permitted on the BlackBerry device, whether the BlackBerry device user tries to download the applications from a web site or link, or the BlackBerry Enterprise Server or another party sends the applications to the BlackBerry device.	False	Java based	3.6	4.0	2.1 4.0	Use this IT policy rule to prevent the BlackBerry device from downloading and installing third-party applications that RIM has not digitally signed.
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			—	—	3.6	—	—
BlackBerry Enterprise Server for Novell GroupWise exceptions:			—	4.0	—	—	—

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
External File System Encryption Level	Specify the level of file system encryption that the BlackBerry device uses to encrypt files that it stores on an external file system: • **0**: do not require file system encryption • **1**: encrypt file system to a user-provided password; exclude multi-media directories) • **2**: encrypt file system to a user-provided password; include multi-media directories • **3**: encrypt file system to the BlackBerry device key; exclude multi-media directories • **4**: encrypt file system to the BlackBerry device key; include multi-media directories • **5**: encrypt file system to a user-provided password and the BlackBerry device key; exclude multi-media directories • **6**: encrypt file system to a user-provided password and the BlackBerry device key; include multi-media directories	0	Java based	4.2	4.0.6	—	You can use this IT policy rule to require the BlackBerry device to encrypt an external file system, either including or excluding multi-media directories. **Note**: The external file system encryption does not apply to files that the BlackBerry device user manually transfers to the external memory device (for example, from a USB mass storage device). The external memory device stores the media card master 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 either the BlackBerry device key, a user-provided password, or both to encrypt the master keys.

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
FIPS Level	Specify the level of Federal Information Processing Standard (FIPS) compliance. • **1**: FIPS 140-2 Level 1 compliance • **2**: FIPS 140-2 Level 2 compliance Level 1 compliance affects the BlackBerry Cryptographic Kernel, which is the embedded cryptographic module required for basic operation of the BlackBerry device. Level 2 compliance affects only the BlackBerry device software and does not result in the BlackBerry device meeting FIPS 140-2 Level 2 hardware security requirements. If you set this IT policy rule to 2, the BlackBerry device prevents WTLS from using a Rivest cipher (RC5), which can cause problems using the WTLS protocol.	1	Java based	3.3.0 to support Level 1 compliance 4.0.0 to support Level 2 compliance	4.0	4.0	**Rule dependency**: If you set this IT policy rule to 2, the following additional rules are enforced • Password Required = True • Minimum Password Length = 5 • Suppress Password Echo = True • PGP Allowed Content Ciphers = AES (256-bit), AES (192-bit), AES (128-bit), Triple DES • S/MIME Allowed Content Ciphers = AES (256-bit), AES (192-bit), AES (128-bit), Triple DES • TLS Restrict FIPS Ciphers = True • Disallow Third Party Application Download = True
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Java based only	4.0	—	—	—

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Firewall Block Incoming Messages	Specify whether or not the firewall on the BlackBerry device blocks, and prevents the BlackBerry device from processing, specific types of incoming messages. Specify whether or not the firewall on the BlackBerry device blocks, and prevents the BlackBerry device from processing, specific types of incoming messages that bypass your corporate network: • SMS Messages • MMS Messages • BlackBerry Internet Service Messages • PIN Messages (Public) • PIN Messages (Corporate) **Note**: The default peer-to-peer encryption key is used to send public PIN messages that are known to all BlackBerry devices. A BlackBerry device with a corporate peer-to-peer encryption key can send and receive corporate PIN messages with other BlackBerry devices on your corporate network with the same peer-to-peer encryption key only.	–	Java based	4.2	4.0.6	–	If you set this IT policy rule, the BlackBerry device drops the specified type(s) of incoming messages at the firewall and does not display received message notifications for those messages. **Note**: Users can specify whether or not to block public PIN messages on the BlackBerry device. Users cannot specify whether or not to block corporate PIN messages on the BlackBerry device

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Force Content Protection of Master Keys	Specify whether or not content protection of master keys that the BlackBerry device stores is turned on.	False	Java based	4.1.0	4.0.3	—	Content protection of master encryption keys encrypts the master encryption keys stored on the BlackBerry device in flash memory using 256-bit AES.
Force Include Address Book In Content Protection	Specify whether or not the Include Address Book option in the General Security Options screen on the BlackBerry device is turned on or off. By default, when you turn on or the user turns on content protection on the BlackBerry device, the BlackBerry device is designed to encrypt the user data on the BlackBerry device when the BlackBerry device is locked but the user can choose to turn on or off content protection for their address book specifically.	False (The Caller ID and Bluetooth Address Book transfer features are permitted to work when content protection is turned on and the BlackBerry device is locked.)	Java based	4.2	4.0.6	—	Set this IT policy rule to True to require that content protection, if turned on, protects the address book on the BlackBerry device when the BlackBerry device is locked, and the user cannot turn off the Include Address Book option. The Caller ID and Bluetooth Address Book transfer features will not work when the BlackBerry device is locked.
Force LED Blinking When Microphone Is On	Specify whether or not the BlackBerry device LED blinks when the microphone is on (for example, when a phone call is in progress or a voice message is recording).	False	Java based	4.1.0	4.0.3	—	—
Force Lock When Holstered	Specify whether or not the BlackBerry device is security-locked when the user places it in the holster.	False	Java based	3.6	4.0	4.0	—
BlackBerry Enterprise Server for Novell GroupWise exceptions:			—	4.0	—	—	—

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Force Smart Card Two Factor Authentication	Specify whether or not the user must type the BlackBerry device password and the smart card password to use the BlackBerry device.	False	Java based	3.6	4.0	4.0	If you set this IT policy rule to True, users might require a smart card authenticator module and must have a smart card driver and a BlackBerry Smart Card Reader driver installed on their BlackBerry devices, to use their BlackBerry devices. **Rule dependency**: If you set this IT policy rule to True, the BlackBerry Enterprise Server automatically sets the Password Required rule to True in the same BlackBerry device IT policy. You must manually set the Password Required rule to True for BlackBerry devices running BlackBerry Device Software versions earlier than 4.2.
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	3.6	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			–	4.0	–	–	–

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Force Smart Card Two Factor Challenge Response	Specify whether or not the user must choose a smart card certificate for use with smart card two factor authentication. If you set this IT policy rule to True, when the user unlocks the BlackBerry device, the BlackBerry device sends a challenge to the smart card to verify that the BlackBerry device used to initialize the authenticator module. This feature increases smart card two factor authentication, but the BlackBerry device requires more time to unlock.	False	Java based	4.2	4.0.6	–	If you set this IT policy rule, to True, users must have a BlackBerry Smart Card Reader, and a smart card driver and BlackBerry Smart Card Reader driver installed on their BlackBerry devices. **Rule dependency**: The BlackBerry device uses this IT policy rule only if you set the Password Required and Force Smart Card Two Factor Authentication rules to True.
Key Store Password Maximum Timeout	Specify the maximum number of minutes the BlackBerry device allows to elapse before the cached key store password times out and the BlackBerry device prompts the user to type the password.	1	Java based	3.6	4.0	4.0	If you set this IT policy rule to 0, the BlackBerry device cannot cache the key store password to reduce the number of times that the BlackBerry device prompts the user for the password.
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	3.6	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			–	4.0	–	–	–

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Lock on Smart Card Removal	Specify whether or not the BlackBerry device locks when the user removes the paired smart card from the BlackBerry Smart Card Reader or disconnects the BlackBerry Smart Card Reader from the BlackBerry device. **Warning**: Not all smart card reader drivers support smart card removal detection.	False	Java based	3.6	4.0	4.0	If you set this IT policy rule to True, users might require a smart card authenticator module and must have a smart card driver and a BlackBerry Smart Card Reader driver installed on their BlackBerry devices, to use their BlackBerry devices. **Rule dependency**: If you set this IT policy rule to True, the BlackBerry Enterprise Server automatically sets the Password Required and Force Smart Card Two Factor Authentication rules to True in the same BlackBerry device IT policy.
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	3.6	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			–	4.0	–	–	–
Message Classification	Specify the set of message classifications available to users to apply to email messages sent using the BlackBerry Enterprise Server.	–	Java based	4.2	4.1.2	–	–

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Minimal Encryption Key Store Security Level	Specify the minimum security level for the private key in the key store to be accessed for encrypting messages. • **Low security**: The BlackBerry device never prompts the user for the key store password when accessing the private key for encrypting messages. • **High security**: The BlackBerry device always prompts the user for the key store password. If the user recently typed the password, the BlackBerry device prompts the user to confirm the password to access the private key for encrypting messages. • **Medium security**: The BlackBerry device only prompts the user for the key store password if the password is cleared from the key store cache.	Medium security	Java based	4.0	4.0	4.0	The BlackBerry device forces all keys to use the security level you set as the minimum, but the user can set a higher security level on the BlackBerry device.

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Minimal Signing Key Store Security Level	Specify the minimum security level for the private key in the key store to be accessed for signing messages. • **Low security**: The BlackBerry device never prompts the user for the key store password when accessing the private key for signing messages. • **High security**: The BlackBerry device always prompts the user for the key store password. If the user recently typed the password, the BlackBerry device prompts the user to confirm the password to access the private key for signing messages. • **Medium security**: The BlackBerry device only prompts the user for the key store password if the password is cleared from the key store cache.	Medium security	Java based	4.0	4.0	4.0	The BlackBerry device forces all keys to use the security level you set as the minimum, but the user can set a higher security level on the BlackBerry device.

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Required Password Pattern	Specify the permitted structure of the BlackBerry device password. Use the following characters in the password pattern to specify the character type permitted in its position in the password: **a**: Permits any letter. **A**: Permits an uppercase letter only. **c**: Permits any consonant letter. **C**: Permits an uppercase consonant letter 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. **Note**: Password characters are restricted to the Latin-1 character set.	–	Java based	4.2	4.0.6	–	If you set this IT policy rule, the user can set a password greater than or equal to the length of the pattern on their BlackBerry device. Password characters that exceed the pattern length can be any letters, numbers, or symbols. **Warning**: Preventing a particular password character reduces the entropy level and security level of the password.
Require Secure APB Messages	Specify whether or not the BlackBerry device can receive insecure messages, including All Points Bulletin (APB) messages, from a BlackBerry Enterprise Server.	False	Java based	4.2	4.0.6	–	The BlackBerry device can receive all messages from the BlackBerry Enterprise Server that are not blocked at the firewall unless you set this IT policy to True to prevent the BlackBerry device from receiving insecure messages.

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Secure Wipe Delay After IT Policy Received	Specify the length of time, in hours, after receiving an IT policy update that the BlackBerry device securely wipes all of its user data. The permitted range is 2 to 720 hours. **Warning**: If you set this IT policy rule, set the Policy Resend Interval on the BlackBerry Enterprise Server (in the IT Admin properties) to a value that is lower than this rule setting to prevent unwanted BlackBerry device wiping.	—	Java based	4.2	4.0.6	—	Use this IT policy rule to require a BlackBerry device that cannot receive IT policy updates or IT Admin commands to perform a secure wipe of user data after a specified length of time.
Secure Wipe Delay After Lock	Specify the length of time, in hours, after the BlackBerry device locks that the BlackBerry device securely wipes all of its user data. The permitted range is 2 to 720 hours.	—	Java based	4.2	4.0.6	—	Use this IT policy rule to require a BlackBerry device that the user has not unlocked within the length of time specified to perform a secure wipe of user data.
Secure Wipe if Low Battery	Specify whether or not the BlackBerry device securely wipes all of its user data if the BlackBerry device battery becomes critically low.	False	Java based	4.2	4.0.6	—	Use this IT policy rule to require a BlackBerry device with insufficient battery power to receive IT policy updates or IT Admin commands to perform a secure wipe of user data after the length of time specified.

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Security Service Colors	Specify the background color of two message types, in RGB, hexadecimal format. The first color represents the background color of messages sent using the same BlackBerry Enterprise Server that sent the IT policy. The second color represents the background color of messages from other services (for example, from a web client).	—	Java based	4.0	4.0	4.0	Example colors: • 0xffffff: white • 0x000000: black • 0xff0000: red • 0x00ff00: green • 0x0000ff: blue
Trusted Certificate Thumbprints	Specify a string that contains a semi colon-separated list of Hex-ASCII certificate thumbprints, generated using either a Secure Hash Algorithm (SHA-1) or Message-Digest algorithm 5 (MD5).	—	Java based	3.6	4.0	4.0	If this string is present, the user can only add certificates with thumbprints that appear in the defined list to the trusted key store.
BlackBerry Enterprise Server for Novell GroupWise exceptions:			—	4.0	—	—	—

Service Exclusivity policy group

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Allow Other Browser Services	Specify whether or not the BlackBerry device permits other browser services.	True	Java based	3.6	4.0	4.0 (internal)	Set this IT policy rule to False to force browser traffic through your company's BlackBerry Enterprise Server and to prevent users from installing other browser services.
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	3.5	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			–	4.0	–	–	–
Allow Other Message Services	Specify whether or not the BlackBerry device permits other email message services.	True	Java based or C++-based	3.6 (Java based BlackBerry device) or 2.5 (C++-based BlackBerry device)	4.0	4.0 (internal)	Set this IT policy rule to False to force outbound email messages through your company's BlackBerry Enterprise Server and to prevent users from sending outbound email messages using other message services. **Warning**: This IT policy rule does not prevent users from receiving inbound messages from other message services.
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	3.5	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Java based only	4.0	–	–	–

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Allow Public AIM Services	Specify whether or not AOL® Instant Messenger (AIM®) for BlackBerry services are permitted on the BlackBerry device.	True	Java based or C++-based	3.6 (Java based BlackBerry device) or 2.5 (C++-based BlackBerry device)	4.0.3	—	Set this IT policy rule to False to prevent AIM activity through the BlackBerry Enterprise Solution™.
Allow Public Google Talk Services	Specify whether or not Google Talk for BlackBerry services are permitted on the BlackBerry device.	True	Java based only	3.6 (Java based BlackBerry device)	4.1	—	Set this IT policy rule to False to prevent Google™ Talk instant message activity through the BlackBerry Enterprise Solution. **Note**: If you set this IT policy rule to False and users have downloaded Google Talk for BlackBerry onto their BlackBerry devices, the Google Talk for BlackBerry icon remains on the Home screen. If users attempt to sign into Google Talk for BlackBerry, a message on their BlackBerry device indicates that they cannot use Google Talk for BlackBerry.

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Allow Public ICQ Services	Specify whether or not ICQ® for BlackBerry services are permitted on the BlackBerry device.	True	Java based or C++-based	3.6 (Java based BlackBerry device) or 2.5 (C++-based BlackBerry device)	4.0.3	–	Set this IT policy rule to False to disable access to ICQ for BlackBerry services.
Allow Public IM Services	Specify whether or not public Instant Messaging (IM) for BlackBerry services are permitted on the BlackBerry device.	True	Java based or C++-based	3.6 (Java based BlackBerry device) or 2.5 (C++-based BlackBerry device)	4.0.3	–	Set this IT policy rule to False to disable access to public IM services for BlackBerry services. **Note**: This policy is respected by all RIM public IM services that were released after the first availability of this policy rule. Yahoo!® Messenger 1.0 is controlled by a separate IT policy rule.
Allow Public Yahoo! Messenger Services	Specify whether Yahoo! Messenger for BlackBerry services are permitted on the BlackBerry device.	True	Java based or C++-based	3.6 (Java based BlackBerry device) or 2.5 (C++-based BlackBerry device)	4.0	4.0	Set this IT policy rule to False to disable access to Yahoo! Messenger for BlackBerry services.
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	3.5	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Java based only	4.0	–	–	–

SIM Application Toolkit policy group

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Disable Network Location Query	Specify whether or not the network or subscriber identity module (SIM) can query the BlackBerry device for certain location-related information.	False	Java based	3.6	– S/MIME Support Package version 4.0	4.0	The information that the SIM can query is limited to current network and cell identities, the BlackBerry device International Mobile Equipment Identity (IMEI), the date, time, and some measurement results.
BlackBerry Enterprise Server for Novell GroupWise exceptions:			–	4.0	–	–	–
Disable SIM Call Control	Specify whether or not the SIM can modify an outgoing call, supplementary service request, or short message.	False	Java based	3.6	– S/MIME Support Package version 4.0 or later	4.0	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported	Not supported	Not supported	–	–
Disable SIM Originated Calls	Specify whether or not the SIM can make an outgoing call, perform a supplementary service operation, or send a short message.	False	Java based	3.6	– S/MIME Support Package version 4.0 or later	4.0	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			Not supported	Not supported	Not supported	–	–

Smart Dialing policy group

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
Enable Smart Dialing Policy	Specify whether or not smart dialing on Voice over Internet Protocol (VoIP) calls is enabled on the BlackBerry device.	True	Java based	4.0	4.0.1	Not applicable	–
Set Local Area Code	Specify the local area code.	–	Java based	4.0	4.0.1	–	**Rule dependency**: The BlackBerry device uses this IT policy rule only if you set the Enable Smart Dialing rule to True.
Set Local Country Code	Specify the local country code.	–	Java based	4.0	4.0.1	–	**Rule dependency**: The BlackBerry device uses this IT policy rule only if you set the Enable Smart Dialing rule to True.
Set National Number Length	Specify the national phone number length.	–	Java based	4.0	4.0.1	–	**Rule dependency**: The BlackBerry device uses this IT policy rule only if you set the Enable Smart Dialing rule to True.
Smart Dialing Allow Device Changes	Specify whether or not the user can configure Smart Dialing settings on the BlackBerry device.	True	Java based	4.0	4.0.1	–	This IT policy rule permits users to set Smart Dialing settings for remote troubleshooting. **Rule dependency**: The BlackBerry device uses this IT policy rule only if you set the Enable Smart Dialing rule to True.

TCP policy group

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
TCP APN	Specify whether or not a default Access Point Name (APN) can be imposed on the BlackBerry device when it uses the Transmission Control Protocol (TCP).	—	Java based	4.0	4.0	4.0	—
TCP Password	Specify whether or not a default APN password can be imposed on the BlackBerry device when it uses the TCP.	—	Java based	4.0	4.0	4.0	—
TCP Username	Specify whether or not a default APN user name can be imposed on the BlackBerry device when it uses the TCP.	—	Java based	4.0	4.0	4.0	—

TLS policy group

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
TLS Device Side Only	Specify whether or not proxy mode TLS or proxy HTTPS is allowed between the BlackBerry device and the BlackBerry Enterprise Server.	False	Java based	4.0	4.0	4.0	If you set this IT policy rule to True, all HTTPS connections must use device-side TLS. **Warning:** If this IT policy rule has been set and device-side TLS is unavailable, an exception occurs.

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
TLS Disable Invalid Connection	Specify whether or not the BlackBerry device can use connections to servers with invalid certificates during TLS connections. • **0**: turn off invalid connections • **1**: allow invalid connections • **2**: prompt user on the BlackBerry device	2	Java based	3.6.1	4.0	4.0	–
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	3.6	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			–	4.0	–	–	–
TLS Disable Untrusted Connection	Specify whether or not the BlackBerry device can use connections to untrusted servers during a TLS connection. • **0**: disallow untrusted connections • **1**: allow untrusted connections • **2**: prompt user on the BlackBerry device	2	Java based	3.6.1	4.0	4.0	–
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	3.6	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			–	4.0	–	–	–
TLS Disable Weak Ciphers	Specify whether or not the BlackBerry device can use weak ciphers during a TLS connection. • **0**: turn off weak ciphers • **1**: allow weak ciphers • **2**: prompt user on the BlackBerry device	2	Java based	3.6.1	4.0	4.0	–
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	3.6	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			–	4.0	–	–	–
TLS Minimum Strong DH Key Length	Specify the minimum DH key size, in bits, that the BlackBerry device allows for use in the TLS connection.	1024	Java based	3.6.1	4.0	4.0	–
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	3.6	–	–

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
BlackBerry Enterprise Server for Novell GroupWise exceptions:			–	4.0	–	–	–
TLS Minimum Strong DSA Key Length	Specify the minimum DSA key size, in bits, allowed for use in TLS connections.	1024	Java based	3.6.1	4.0	4.0	–
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	3.6	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			–	4.0	–	–	–
TLS Minimum Strong ECC Key Length	Specify the minimum ECC key size, in bits, allowed for use in the TLS connection.	163	Java based	3.6.1	4.0	4.0	–
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	3.6	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			–	4.0	–	–	–
TLS Minimum Strong RSA Key Length	Specify the minimum RSA key size, in bits, allowed for use in TLS connections.	1024	Java based	3.6.1	4.0	4.0	–
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	3.6	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			–	4.0	–	–	–
TLS Restrict FIPS Ciphers	Specify whether or not the BlackBerry device can use a cipher that is not FIPS-compliant with TLS.	False	Java based	3.6.1	4.0	4.0	**Warning**: If the FIPS Level rule is set to 2, the BlackBerry device ignores this IT policy rule and does not use ciphers that are not FIPS-compliant with TLS by default.
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	3.6	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			–	4.0	–	–	–

WTLS policy group

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
WTLS Disable Invalid Connection	Specify whether or not the BlackBerry device can use connections to servers with invalid certificates during WTLS connections. • **0**: turn off invalid connections • **1**: allow invalid connections • **2**: prompt user on the BlackBerry device	2	Java based	3.6	4.0	4.0	–
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	3.6	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			–	4.0	–	–	–
WTLS Disable Untrusted Connection	Specify whether or not the BlackBerry device can use connections to untrusted servers during WTLS connections. • **0**: disallow untrusted connections • **1**: allow untrusted connections • **2**: prompt user on the BlackBerry device	2	Java based	3.6	4.0	4.0	–
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	3.6	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			–	4.0	–	–	–
WTLS Disable Weak Ciphers	Specify whether or not the BlackBerry device can use weak ciphers during WTLS connections. • **0**: turn off weak ciphers • **1**: allow weak ciphers • **2**: prompt user on the BlackBerry device	2	Java based	3.6	4.0	4.0	–
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			–	–	3.6	–	–
BlackBerry Enterprise Server for Novell GroupWise exceptions:			–	4.0	–	–	–
WTLS Minimum Strong DH Key Length	Specify the minimum DH key size, in bits, allowed for use in the WTLS connection.	1024	Java based	3.6	4.0	4.0	–

Policy rule	Description	Default setting	Minimum requirements				Use
			BlackBerry device type	BlackBerry Device Software	BlackBerry Enterprise Server software	BlackBerry Connect Transport Stack	
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			—	—	3.6	—	—
BlackBerry Enterprise Server for Novell GroupWise exceptions:			—	4.0	—	—	—
WTLS Minimum Strong ECC Key Length	Specify the minimum ECC key size, in bits, allowed for use in the WTLS connection.	163	Java based	3.6	4.0	4.0	—
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			—	—	3.6	—	—
BlackBerry Enterprise Server for Novell GroupWise exceptions:			—	4.0	—	—	—
WTLS Minimum Strong RSA Key Length	Specify the minimum RSA key size, in bits, allowed for use in WTLS connections.	1024 bits	Java based	3.6	4.0	4.0	—
BlackBerry Enterprise Server for Microsoft Exchange exceptions:			—	—	3.6	—	—
BlackBerry Enterprise Server for Novell GroupWise exceptions:			—	4.0	—	—	—
WTLS Restrict FIPS Ciphers	Specify whether or not the BlackBerry device can use a cipher that is not FIPS-compliant with WTLS.	False	Java based	4.0	4.0	4.0	**Warning:** If the FIPS Level rule is set to 2, the BlackBerry device ignores this IT policy rule and does not use ciphers that are not FIPS-compliant with WTLS by default.

3

Application control policy rules

Understanding application control policies

Assign application control policy rule values in the application control policy. The BlackBerry Enterprise Server application control policy rules are designed to enable you to permit or prevent the installation of specific third-party applications on the BlackBerry device and to limit the permissions of third-party applications installed on the BlackBerry device.

Defining software configurations

Before you can set an application control policy on a BlackBerry device, you must set up a software configuration and install all of the necessary application files either on the BlackBerry Enterprise Server or on any other computer on which the BlackBerry Enterprise Server administrator tools are installed.

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

If you assign the BlackBerry device a software configuration when upgrading the BlackBerry device software, the software configuration applies successfully only if the BlackBerry device remains connected to the computer running the BlackBerry Device Manager until the upgrade completes. Assign the software configuration after the BlackBerry device software is installed to make sure that the software configuration applies to the BlackBerry device successfully.

Applying application control policies

After you assign a software configuration to a user, the user can connect to the shared application loader and install or upgrade to BlackBerry device software that you assign. To control or change the behavior of third-party applications on the BlackBerry device, you must set an application control policy.

For example, to permit users in your organization to use a trusted application to send and receive data from internal servers, permit the trusted application to make internal connections but prevent all other third-party applications from making internal connections.

You can also set application policy rules for user groups (for example, permit an application to access internal servers for a small subset of trusted users only).

You can apply an application policy to one or more applications (preventing only those applications from doing certain things). If no default application policy is assigned, the user can change application controls on the BlackBerry device. If a default application control policy is assigned (that is, not assigned to a specific application, but set as a default for third-party applications that the BlackBerry device downloads thereafter), the user cannot change application controls.

Application control policy rule descriptions

Rule	Description	Default setting	BlackBerry Enterprise Server software (minimum requirement)
Internal Domains	Specify the internal domain names to which the application can establish a connection.	NULL	4.0
External Domains	Specify the external domain names to which the application can establish a connection.	NULL	4.0
Browser Filter Domains	Specify the list of domains for which the application can apply browser filters to web page content on the BlackBerry device. For example, you can specify google.com and yahoo.com as domains for which an application is permitted to use a search engine browser filter on the BlackBerry device.	NULL	4.0
Disposition	Specify whether the application is optional, required, or not permitted on the BlackBerry device. You can use this rule to require a specific application on the BlackBerry device or prevent an unspecified or untrusted application from being loaded on the BlackBerry device.	Optional	4.0
Interprocess Communication	Specify whether or not the application can perform interprocess communication operations. You can use this rule to prevent two or more applications to share data and for one application to use the connection permissions of another application.	Allowed	4.0
Internal Network Connections	Specify whether or not the application can make internal network connections. You can use this rule to permit or prevent the application from sending or receiving any data on the BlackBerry device using an internal protocol (for example, using corporate MDS, or to require the user to respond to a prompt on the BlackBerry device to permit internal connections through the BlackBerry device firewall.	Prompt User	4.0
External Network Connections	Specify whether or not the application can make external network connections. You can use this rule to permit or prevent the application from sending or receiving any data on the BlackBerry device using an external protocol (for example, using a WAP gateway, public MDS, or TCP), or to require the user to respond to a prompt on the BlackBerry device to permit external connections through the BlackBerry device firewall.	Prompt User	4.0

Rule	Description	Default setting	BlackBerry Enterprise Server software (minimum requirement)
Local Connections	Specify whether or not the application can make local network connections (for example, connections to the BlackBerry device using a USB or serial port).	Allowed	4.0
Phone Access	Specify whether or not the application can make phone calls and access phone logs on the BlackBerry device. You can use this rule to permit or prevent the application from making any calls on the BlackBerry device or to require the user to respond to a prompt on the BlackBerry device to permit the application to make a phone call.	Prompt User	4.0
Message Access	Specify whether or not the application can send and receive messages on the BlackBerry device using the email API.	Allowed	4.0
PIM Data Access	Specify whether or not the application can access the BlackBerry device PIM APIs, which control access to the personal information of the user on the BlackBerry device, including the address book. **Note**: Permitting the application to access PIM data APIs and use internal and external network connection protocols creates an opportunity for an application to send all of the user's personal data from the BlackBerry device.	Allowed	4.0
Browser Filters	Specify whether or not the application can access browser filter APIs to register a browser filter with the browser on the BlackBerry device. You can use this rule to permit third-party applications to apply custom browser filters to web page content on the BlackBerry device.	Not Permitted	4.0
Event Injection	Specify whether or not the application can inject synthetic input events, such as pressing keys and performing trackwheel actions, on the BlackBerry device.	Not Permitted	4.0
Bluetooth Serial Profile	Specify whether or not the application can access the Bluetooth serial port profile API. **Note**: If you set the Disable Serial Port Profile IT policy rule to True, the Bluetooth enabled BlackBerry device cannot use the Bluetooth SPP to establish a serial connection to a Bluetooth enabled device.	Allowed	4.0
BlackBerry Device Keystore	Specify whether or not the application can access the BlackBerry device key store APIs. If you set the Minimal Signing Key Store Security Level and the Minimal Encryption Key Store Security Level IT policy rules to use the high security level, the BlackBerry device prompts the user for their key store password each time an application tries to access their private key, and this application policy control rule is not recognized.	Allowed	4.0

Rule	Description	Default setting	BlackBerry Enterprise Server software (minimum requirement)
BlackBerry Device Keystore Medium Security	Specify whether or not the application can access key store items stored at the medium security level (the default level), which requires the BlackBerry device to prompt the user for their key store password when an application tries to access their private key for the first time or when their private key password timeout expires. If you set the Minimal Signing Key Store Security Level and the Minimal Encryption Key Store Security Level IT policy rules to use the high security level, the BlackBerry device prompts the user for their key store password each time an application tries to access their private key, and this application policy control rule is not recognized.	Allowed	4.0
Device GPS	Specify whether or not the application can access the BlackBerry device Global Positioning System (GPS) APIs. You can use this rule to permit or prevent the application from accessing the GPS APIs on the BlackBerry device or to require the user to respond to a prompt on the BlackBerry device to permit access to the GPS APIs.	Prompt User	4.1
Theme Data	Specify whether or not the custom theme applications developed using the Plazmic Content Developer's Kit (CDK) that are installed on the BlackBerry device can be used as themes on the BlackBerry device.	Allowed	4.1
User Authenticator API	Specify whether or not an application is allowed to access the user authenticator framework API. The user authenticator framework permits the registration of drivers (currently smart card drivers only) that provide two-factor authentication to unlock the BlackBerry device. This application control policy rule applies to BlackBerry device software and third-party Java applications.	Allowed	4.1

4

BlackBerry MDS Services policy rules

Rule	Description	Default setting	BlackBerry Enterprise Server software (minimum requirement)
Allow Runtime Upgrade by User	Specify whether or not users can upgrade the BlackBerry MDS Runtime software on their BlackBerry devices.	False	4.1
Allow Discovery by User	Specify whether or not users can search a BlackBerry MDS Studio Application repository for BlackBerry MDS Studio applications that are on their BlackBerry devices.	True	4.1
Allow Application Install by User	Specify whether or not users can install BlackBerry MDS Studio applications on their BlackBerry devices. The following values are permitted: 0 = Users cannot install BlackBerry MDS Studio applications. 2 = Users can install BlackBerry MDS Studio applications.	2	4.1
Allow Push Application Install	Specify whether or not the BlackBerry Enterprise Server administrator can send BlackBerry MDS Studio applications to the BlackBerry device for installation.	True	4.1
Allow Application Delete by User	Specify whether or not users can delete BlackBerry MDS Studio applications from their BlackBerry devices.	True	4.1
Allow External Access	Specify whether or not BlackBerry MDS Studio applications that are installed on the BlackBerry device can access other applications and data, such as email and calendar, on the BlackBerry device. The following values are permitted: 0 = BlackBerry MDS Studio applications cannot access data from other applications on the BlackBerry device. 1 = BlackBerry MDS Studio applications can retrieve data from other applications on the BlackBerry device. 2 = BlackBerry MDS Studio applications can retrieve data from and send data to other applications on the BlackBerry device.	0	4.1
Allow Access to Multiple Domains	Specify whether or not BlackBerry MDS Studio applications that are installed on the BlackBerry device can access web services in multiple domains.	False	4.1

Rule	Description	Default setting	BlackBerry Enterprise Server software (minimum requirement)
Queue Limit for Inbound Application Messages	Specify the maximum number of messages from BlackBerry MDS Studio applications that can be queued locally on the BlackBerry device. The valid range is from 1 to 50 messages.	8	4.1
Queue Limit for Outbound Application Messages	Specify the maximum number of messages to BlackBerry MDS Studio applications that can be queued locally on the BlackBerry device. The valid range is from 1 to 50 messages.	16	4.1

5

Example IT policies and application control policies

You might consider setting IT policy rules and application control policy rules to define acceptable security and functionality.

Security consideration	Description
user authentication	Use IT policy rules to • require a user to authenticate to the BlackBerry device using a security password • configure features such as password duration, length, and strength • require password patterns • forbid specific passwords
encryption	Use IT policy rules to • extend encryption of data in transit between the sender and recipient of an email or PIN message • enable the BlackBerry device to generate and use the content protection key to encrypt user data while the BlackBerry device is locked • enable the BlackBerry device to generate and use the grand master key to encrypt the master encryption key while the BlackBerry device is locked • specify the level of FIPS compliance for the BlackBerry Cryptographic Kernel, to require a specific standard of encryption strength
application installation and use	Use IT policy rules to • prevent BlackBerry devices from downloading third-party applications over the wireless network • specify whether or not applications, including third-party applications, on the BlackBerry device can initiate specific types of connections

Security consideration	Description
virus and malicious user prevention measures	Use application control policy rules to • specify which resources (for example, email, phone, and BlackBerry device key store) a third-party application can access on the BlackBerry device • specify the types of connections that a third-party application running on the BlackBerry device can establish (for example, local connections, internal connections, and external connections) • specify whether or not an application can access the user authenticator framework API, which permits the registration of drivers to provide two-factor authentication to unlock the BlackBerry device
Bluetooth technology use	Use IT policy rules to • manage all Bluetooth-enabled BlackBerry devices • prevent the use of Bluetooth technology on all Bluetooth-enabled devices by turning off Bluetooth support • specify whether or not the Bluetooth-enabled BlackBerry device can establish a relationship—or pair—with another Bluetooth-enabled device • specify whether or not the user can turn on or turn off the Bluetooth profiles on the BlackBerry device

Define acceptable user authentication

Use IT policy rules to require and define acceptable corporate passwords and passphrases on BlackBerry devices in your organization. When you require a password on the BlackBerry device, users must set a password and type the password correctly to access the applications and data on their BlackBerry devices.

Scenario	Policy rule	Setting
Extend a corporate password policy to BlackBerry devices.	Password Required	True
	Maximum Password Age	30 (days)
	Minimum Password Length	8 (characters)
	Password Pattern Checks	2 (requires at least one alphabetic, one numeric, and one special character)
	Forbidden Passwords	Prevent use of obvious and insecure passwords (for example, "password", usernames, and company name(s))
	Set Password Timeout	5 (minutes)
	User Can Change Timeout	False
Erase all user data on the BlackBerry device if the user types the password incorrectly. **Note**: The maximum number of password attempts is reduced to half the default number of attempts when duress mode is enabled.	Set Maximum Password Attempts	10 (incorrect passwords typed before the BlackBerry device data is erased)
Do not permit users to use the same password repeatedly.	Maximum Password History	10 (maximum number of previous passwords that the new password must be checked against)

Scenario	Policy rule	Setting
Enable users to notify administrators if the BlackBerry device is in jeopardy of theft. **Note**: The user's duress password is the BlackBerry device password with the first character moved to the end (for example, "hello" for the BlackBerry device password becomes "elloh" for the duress password).	Duress Notification Address	Type the email address that receives notification when a user types a password under duress

Define measures to protect the BlackBerry device from unauthorized use

Scenario	Policy rule	Setting
Lock the BlackBerry device automatically (after 60 mins) regardless of user activity. **Note**: If the Periodic Challenge Time rule is set, the default 60 minutes is replaced by the value specified in the Periodic Challenge Time rule.	Enable Long Term Timeout	True
Prompt the user to type a password, regardless of whether the BlackBerry device is idle or is in use.	Periodic Challenge Time	60 (minutes after which the user is prompted to type a password)
Lock the BlackBerry device automatically when a user inserts it in the holster.	Force Lock When Holstered	True
Lock the BlackBerry device automatically after a period of user inactivity.	Maximum Security Timeout	5 (minutes of idle time allowed before the BlackBerry device locks)

Define acceptable encryption of BlackBerry device data

Scenario	Policy rule	Value
Protect user and application data on the BlackBerry device.	Content Protection Strength	True
Protect the master encryption key on a locked BlackBerry device.	Force Content Protection of Master	True
Specify the level of FIPS compliance on the BlackBerry device.	FIPS Level	2
Specify the content ciphers that the BlackBerry device uses to encrypt and decrypt PGP messages.	PGP Allowed Content Ciphers	AES (256-bit), AES (192-bit), AES (128-bit), and Triple DES
Specify the content ciphers that the BlackBerry device uses to encrypt and decrypt S/MIME messages.	S/MIME Allowed Content Ciphers	AES (256-bit), AES (192-bit), AES (128-bit), and Triple DES.

Restrict unsecured messaging

You might want to track communications for security or other purposes. If you require all communication to travel through the enterprise messaging environment, you can use IT policy rules to turn off unsecured PIN and text messaging.

Note: PIN messages are encrypted with Triple DES; however, the key to decrypt the message is available to everyone with a BlackBerry device. Therefore, PIN messages should be considered scrambled but not encrypted.

Scenario	Policy rule	Setting
Make sure that all electronic communication between your employees and their clients is recorded to comply with industry regulations.	Allow Other Browser Services	False
	Allow Other Message Services	False
	Allow Peer-to-Peer Messages	False
	Allow SMS	False
	Disable Forwarding Between Services	True
	Disable Cut/Copy/Paste	True
Prevent users from sending PIN messages. **Note**: Users can still receive PIN messages.	Allow Peer-to-Peer Messages	False
Prevent users from sending SMS messages. **Note**: Users can still receive SMS messages.	Allow SMS	False
Prevent users from forwarding or replying to messages using a different BlackBerry Enterprise Server.	Disable Forwarding Between Services	True
Set message sensitivity using different message background colors. **Note**: The background color of messages sent from the BlackBerry Enterprise Server that sent the IT policy is different from the background color of messages sent from other networks (and BlackBerry Enterprise Servers).	Security Service Colors	Type the colors of sensitive and non-sensitive messages in RGB (hexadecimal) format.

Define virus and malicious user prevention measures

The BlackBerry Enterprise Server provides two methods that you can use to limit how a user can install and use third-party applications on the BlackBerry device:

- Set the Disallow Third Party Application Download IT policy rule to True to prevent BlackBerry devices from downloading third-party applications over the wireless network.

Note: If you set the Disallow Third Party Application Download IT policy rule to True, previously installed applications are not removed from the BlackBerry devices.

- Set application control policy rules to require or prevent the installation of specific third-party applications and to control the behavior of third-party applications on BlackBerry devices.

By default, BlackBerry devices can install all third-party applications until you use one or both of these methods to control third-party applications on BlackBerry devices.

Consider the following scenarios and IT policy rule and application control rule settings to limit user control of third-party applications on BlackBerry devices.

Scenario	Application control policy rule setting	IT policy rule
Prevent third-party application access to serial ports or USB ports on the BlackBerry device.	—	Set Allow Third Party Apps to Use Serial Port to False
Prevent third-party application access to the RIM persistent store API.	—	Set Allow Third Party Apps to Use Persistent Store to False
Prevent users from configuring and executing desktop add-ins (for example, third-party COM-based extensions that access the BlackBerry device databases during synchronization).	—	Set Desktop Allow Desktop Add-Ins to False.
Prevent third-party applications or themes from being downloaded to the BlackBerry device.	—	Set Disallow Third Party Application Downloads to True
Prevent the user from removing an installed third-party Java application from a BlackBerry device.	Set Disposition to Required.	—
Prevent the user from loading a third-party Java application onto a BlackBerry device.	Set Disposition	—
Remove a third-party Java application from a BlackBerry device over the wireless network.	Set Disposition	—
Prevent a user from activating a custom theme created using the BlackBerry Plazmic CDK and installed on the BlackBerry device.	Set Theme Data	—
Prevent a user from unlocking the BlackBerry device using a BlackBerry Smart Card Reader and authentication password.	Set User Authenticator API	—
Prevent a user from authenticating through a VPN connection using third-party applications on the BlackBerry device.	Set User Authenticator API	—

Consider the following scenarios and IT policy rule and application control rule settings to limit the resources that installed third-party Java applications can access on BlackBerry devices.

Scenario	Rule	Setting
Prevent the user from removing an installed third-party Java application from a BlackBerry device.	Disposition	Required
Prevent the user from loading a third-party Java application onto a BlackBerry device.	Disposition	Disallowed
Permit a third-party Java application on the BlackBerry device to connect to the internal domain to access internal resources behind the corporate firewall and enable internal network connections from the BlackBerry device (for example, to the BlackBerry MDS Services) by prompting for a password on the BlackBerry device.	Internal Network Connections	Prompt User
	Internal Domains	Type the address of the internal company domain
Prevent a third-party Java application from accessing a list of domains using the BlackBerry Browser.	Browser Filter Domains	Type the address of the domains

Scenario	Rule	Setting
Permit a third-party Java application to send and receive messages on a BlackBerry device.	Message Access	Allowed
Remove a third-party Java application from a BlackBerry device over the wireless network.	Disposition	Disallowed
Permit a third-party Java application (for example, a customer relationship management application) to access the phone application on the BlackBerry device.	Phone Access	Allowed
Permit a third-party Java application to create public external network connections (for example, using TCP, Bluetooth, or WAP Browser) and permit a connection to external domains without prompting the user for a password on the BlackBerry device.	External Network Connections	Allowed
	External Domains	Type the address of the external domains
Permit a third-party Java application to establish connections to a Bluetooth-enabled device.	Bluetooth Serial Profile	Allowed
	External Network Connections	Allowed
Prevent a user from activating a custom theme created using the BlackBerry Plazmic CDK and installed on the BlackBerry device.	Theme Data	Disallowed
Prevent a user from unlocking the BlackBerry device using a BlackBerry Smart Card Reader and authentication password.	User Authenticator API	Disallowed

Example application control policies

Before you set up a software configuration and apply application control policies, on a computer with the BlackBerry Manager available you must perform the following actions:

- create a shared network directory with Read permissions for Everyone
- add a directory to which developers can copy third-party application installation files
- index all of the third-party applications in that location to enable the BlackBerry Infrastructure to register the third-party applications

See the *BlackBerry Enterprise Server System Administration Guide* for more information on making device software and applications available to users.

Set an application control policy to block all third-party applications

Setting the Disallow Third Party Application Download IT policy rule to True to prevent BlackBerry devices from downloading third-party applications over the wireless network does not remove existing third-party applications on the BlackBerry device. To block all third-party applications, set a default application policy that blocks third-party applications from running on a BlackBerry device.

This means that even if a user connects a BlackBerry device with third-party applications installed to a BlackBerry Enterprise Server, the third-party applications are not permitted to run. The new application policy is assigned to the user and the application is unavailable to the user on the BlackBerry device (the software remains on the BlackBerry device, but the software cannot run). If the user tries to install additional third-party applications, the installation will fail and the BlackBerry device will display an authorization failure message.

1. Open the BlackBerry Manager and navigate to the Software Configuration Screen.
2. Click **Manage Application Policies**.
3. Click **New**. Assign any name to the application control policy.
4. Set Disposition to **Disallowed** to remove all existing third-party applications from the BlackBerry device and prevent the BlackBerry device from installing any new third-party applications.
5. Select a software configuration. Click **Edit Configuration**. All available device software series are listed.
6. Apply the application control policy to the default application software for all BlackBerry devices or to a specific BlackBerry device series.
7. Click **OK**.

Set an application control policy to permit a specific, permitted application

If you want to permit (whitelist) a specific third-party application to run on BlackBerry devices, you can use an application control policy that blocks all third-party applications as the default application control policy but register a third-party application in the shared folder and allow that third-party application only. When the user tries to download third-party application software on the BlackBerry device, the download fails for all application software other than the specific application that is allowed by the new application control policy.

1. Open the BlackBerry Manager and navigate to the Software Configuration Screen.
2. Click **Edit Configuration**. The registered application is listed in the software configuration.
3. Click **Manage Application Policies**.
4. Click **New** to create a new application control policy. Assign it any name.
5. Set Disposition to **Optional** to allow the third-party application.

Note: You can also set Disposition to **Required** and then set the Delivery method to **Wireless** in the software configuration to push the application to BlackBerry devices over the wireless network automatically.

6. In the software configuration, assign the new application control policy to the registered third-party application. Leave the application control policy that blocks all third-party applications as the default application control policy.

Assign a default application control policy to control application behavior

If you want to block certain potential application threats instead of banning all third-party applications on BlackBerry devices, you can replace a default application control policy that blocks all third-party applications with a less restrictive application control policy that controls installed third-party application behavior. You can permit the registered application to work while preventing other applications from exchanging data. The registered third-party application still has its assigned permissions, and the user can still install other third-party applications, but those other applications are not permitted to do anything on the BlackBerry device by default.

1. Open the BlackBerry Manager and navigate to the Software Configuration Screen.
2. Click **Edit Configuration**. The registered application is listed in the software configuration.

3. Click **Manage Application Policies**.
4. Click **New** to create a new application control policy. Assign it any name.
5. Set Disposition to **Optional** to allow the third-party application. Do not permit the application to do anything else. Applications that do not require data access (Internet, intranet, or BlackBerry device data), for example, card games or calculators, can still run on the BlackBerry device with these restrictions.
6. Assign the application control policy as the default application control policy.

Published in Canada.