BlackBerry Enterprise Server Express

Version: 5.0
Service Pack: 4

Policy Reference Guide

BlackBerry

Published: 2012-08-17
SWD-20120817105306703

Contents

Related resources

1

To read the following guides or additional related material, visit www.blackberry.com/go/serverdocs .

Guide	Information
What's New in BlackBerry Enterprise Server Express 5.0 SP4 Job Aid	• Summary of new features
BlackBerry Enterprise Server Express Update Guide	• Summary of updates to the administrator guides for BlackBerry Enterprise Server Express 5.0 SP4
BlackBerry Enterprise Server Express Release Notes	• Description of known issues and potential workarounds
BlackBerry Enterprise Server Express Installation and Configuration Guide	• System requirements • Installation instructions
BlackBerry Enterprise Server Express Upgrade Guide	• System requirements • Upgrade instructions

New in this release

2

New configuration setting

Profile type	Setting	BlackBerry Device Software minimum requirement
VPN	Associated Certificate Authority Configuration	5.0

New application control policy rules

Rule	BlackBerry Device Software minimum requirement
Is Access to the Near Field Communication (NFC) Allowed	7.0
Is Access to the Secure Element Allowed	7.0

IT policies

3

You can assign IT policies to BlackBerry devices to meet the security requirements of your organization and the needs of BlackBerry device users. For example, you can create an IT policy, configure the IT policy rules to meet security requirements, add users to a group, and assign the IT policy to the group.

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

Default IT policy

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

Default values for IT policy rules

IT policy group	IT policy rule	Default value
Device Only Items	Allow Peer-to-Peer Messages	Yes
Device Only Items	Allow SMS	Yes
Device Only Items	Enable Long-Term Timeout	Yes
Device Only Items	Enable WAP Config	Yes
Device Only Items	Maximum Password Age	Null value
Device Only Items	Maximum Security Timeout	Null value
Device Only Items	Minimum Password Length	Null value

IT policy group	IT policy rule	Default value
Device Only Items	Password Pattern Checks	No restriction
Device Only Items	Password Required	No
Device Only Items	User Can Change Timeout	Yes
Device Only Items	User Can Disable Password	Yes
Global Items	Allow Browser	Yes
Global Items	Allow Phone	Yes
BlackBerry App World	Enable Wireless Service Provider Billing	No
Bluetooth	Disable Bluetooth	No
Bluetooth	Disable Wireless Bypass	Yes
Browser	Disable JavaScript in Browser	No
Browser	MDS Browser Domains	Null value
Camera	Disable Photo Camera	No
Camera	Disable Video Camera	No
Common	Disable MMS	No
Common	Disable Voice Note Recording	No
Email Messaging	Confirm External Image Download	No
Email Messaging	Disable Manual Download of External Images	No
Email Messaging	Disable Notes Native Encryption Forward and Reply	No
Email Messaging	Disable Rich Content Email	No
Email Messaging	Maximum Native Attachment MFH attachment size	3,145,728 bytes (3 MB)
Email Messaging	Maximum Native Attachment MFH total attachment size	5 MB
Email Messaging	Maximum Native Attachment MTH attachment size	10,240 KB
Email Messaging	Notes Native Encryption Password Timeout	-1
Email Messaging	Require Notes Native Encryption for Outgoing Messages	No

IT policy group	IT policy rule	Default value
Password	Forbidden Passwords	Null value
Password	Maximum Password History	0
Password	Periodic Challenge Time	Yes (60 minutes)
Password	Set Maximum Password Attempts	10
Password	Set Password Timeout	2 minutes (BlackBerry Device Software versions earlier than 4.7) 30 minutes (BlackBerry Device Software 4.7 and later)
Password	Suppress Password Echo	Yes
Personal Devices	Disable Forwarding of Work Content Using Personal Channels	No
Personal Devices	Enable Separation of Work Content	No
Personal Devices	Require Work Resources for Conducting Work Activities	No
Personal Devices	Work Domains	Null value
PIM Synchronization	Disable All Wireless Synchronization	No
PGP Application	PGP Allowed Content Ciphers	Use all supported algorithms
PGP Application	PGP Allowed Encrypted Attachment Mode	Automatic
PGP Application	PGP Allowed Encryption Types	Both
PGP Application	PGP Force Digital Signature	No
PGP Application	PGP Force Encrypted Messages	No
PGP Application	PGP Minimum Strong DH Key Length	1024 bits
PGP Application	PGP Minimum Strong DSA Key Length	1024 bits
PGP Application	PGP Minimum Strong RSA Key Length	1024 bits
PGP Application	PGP More All And Send Mode	Manual

IT policy group	IT policy rule	Default value
PGP Application	PGP Universal Enrollment Method	Email-based enrollment
PGP Application	PGP Universal Policy Cache Timeout	24 hours
PGP Application	PGP Universal Server Address	Null value
RIM Value-Added Applications	Disable Organizer Data Access for Social Networking Applications	Yes
Security	Allow External Connections	Yes
Security	Allow Resetting of Idle Timer	No
Security	Allow Split-Pipe Connections	No
Security	Allow Third Party Apps to Use Serial Port	Yes
Security	Content Protection Strength	Null value
Security	Disable 3DES Transport Crypto	No
Security	Disable External Memory	No
Security	Disable GPS	No
Security	Disable IP Modem	No
Security	Disable USB Mass Storage	No
Security	Disallow Third Party Application Downloads	No
Security	Encryption on On-Board Device Memory Media Files	Allowed
Security	External File System Encryption Level	Not required
Security	Force Lock When Holstered	No
Security	Required Password Pattern	Null value
Security	Reset to Factory Defaults on Wipe	No
Security	Security Transcoder Cod File Hashes	Null value
S/MIME Application	Entrust Messaging Server Email Address	Null value
S/MIME Application	S/MIME Allowed Content Ciphers	Use all supported algorithms

IT policy group	IT policy rule	Default value
S/MIME Application	S/MIME Allowed Encrypted Attachment Mode	Automatic
S/MIME Application	S/MIME Allowed Encryption Types	Both
S/MIME Application	S/MIME Force Digital Signature	No
S/MIME Application	S/MIME Force Encrypted Messages	No
S/MIME Application	S/MIME Minimum Strong DH Key Length	1024 bits
S/MIME Application	S/MIME Minimum Strong DSA Key Length	1024 bits
S/MIME Application	S/MIME Minimum Strong ECC Key Length	163 bits
S/MIME Application	S/MIME Minimum Strong RSA Key Length	1024 bits
S/MIME Application	S/MIME More All and Send Mode	Manual
VPN	VPN User Name	Null value
VPN	VPN User Password	Null value
Wi-Fi	Disable Wi-Fi	No
Wired Software Updates	Allow Web-Based Software Loading	No
Wired Software Updates	Cryptographic Services Backup	Yes
Wireless Software Upgrades	Disallow Patch Download Over Roaming WAN	No

IT policy rules

4

The BlackBerry Enterprise Server Express includes IT policy rules that you can configure to meet the security requirements of your organization and the needs of BlackBerry device users.

Device Only policy group

Allow Peer-to-Peer Messages IT policy rule

Description	This rule specifies whether a BlackBerry device user can send PIN messages. This rule does not prevent the user from receiving PIN messages.
Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP2

Allow SMS IT policy rule

Description	This rule specifies whether a BlackBerry device user can send SMS text messages. This rule does not prevent the user from receiving SMS messages. This rule does not prevent the user from sending and receiving MMS messages. To prevent the user from sending and receiving MMS messages, you can use the Disable MMS IT policy rule.

Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

Enable Long-Term Timeout IT policy rule

Description	This rule specifies whether a BlackBerry device locks after a predefined period of time, regardless of whether the BlackBerry device user is using the device.
Related rules	The Periodic Challenge Time IT policy rule affects this rule. Use the Periodic Challenge Time IT policy rule to shorten or extend the timeout interval.
Possible values	• Yes • No
Default values	• No in the Default IT policy
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP2

Enable WAP Config IT policy rule

Description	This rule specifies whether a BlackBerry device user can use the WAP Browser on a BlackBerry device. If you turn off the WAP Browser and your organization's network service provider uses the WAP service for MMS messaging, you turn off the ability to send and receive MMS messages.

Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP3

Maximum Password Age IT policy rule

Description	This rule specifies the number of days before a BlackBerry device password expires and a BlackBerry device user must set a new password. If you configure this rule to 0, the device password does not expire.
Related IT policy rules	The Password Required IT policy rule affects this rule. A device uses this rule only if the Password Required IT policy rule is configured to Yes.
Possible values	• 0 to 65,535 days
Default values	• 0 days in the Default IT policy
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

Maximum Security Timeout IT policy rule

Description	This rule specifies the maximum time that a BlackBerry device user can specify as the security timeout value. The security timeout value is the number of minutes of inactivity before the BlackBerry device locks.
Related rules	The Password Required IT policy rule affects this rule. A device uses this rule only if the Password Required IT policy rule is configured to Yes.

	The User Can Change Timeout IT policy rule affects this rule. A user can specify any timeout value that is less than the maximum value, unless you configure the User Can Change Timeout IT policy rule to No.
Possible values	• 10 to 480 minutes
Default values	• Null value in the Default IT policy
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

Minimum Password Length IT policy rule

Description	This rule specifies the minimum number of characters that are required for a BlackBerry device password. This rule does not control the maximum number of characters for the password. The maximum number is 32 characters.
Related rules	The Password Required IT policy rule affects this rule. A device uses this rule only if the Password Required IT policy rule is configured to Yes.
Possible values	• 4 to14 characters
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

Password Pattern Checks IT policy rule

Description	This rule specifies whether to verify that a BlackBerry device password matches specific character-pattern requirements. By default, a device prevents a BlackBerry device user from

	setting a password that uses a natural sequence of characters or numbers. If a symbol is inserted into a natural sequence, a device can use the password.
Related rules	The Password Required IT policy rule affects this rule. A device uses this rule only if the Password Required IT policy rule is configured to Yes.
Possible values	• At least 1 alpha and 1 numeric character • At least 1 alpha, 1 numeric, and 1 special character • At least 1 upper-case alpha, 1 lower-case alpha, 1 numeric, and 1 special character • No restriction
Default values	• No restriction in the Default IT policy
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

Password Required IT policy rule

Description	This rule specifies whether a BlackBerry device user must configure a password on a BlackBerry device.
Possible values	• Yes • No
Default values	• No in the Default IT policy
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

User Can Change Timeout IT policy rule

Description	This rule specifies whether a BlackBerry device user can override the security timeout value.
Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

User Can Disable Password IT policy rule

Description	This rule specifies whether a BlackBerry device user can turn off the requirement for a password on a BlackBerry device. This rule is obsolete for BlackBerry Device Software 4.0 or later.
Related rules	The Password Required IT policy rule affects this rule. A device uses this rule only if the Password Required IT policy rule is configured to Yes.
Possible values	• Yes • No
Default values	• Yes in the Default IT policy
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

Global policy group

Allow Browser IT policy rule

Description	This rule specifies whether the BlackBerry Browser is available on a BlackBerry device. This rule does not affect other browsers.
Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP2

Allow Phone IT policy rule

Description	This rule specifies whether the phone is available on a BlackBerry device.
Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP2

BlackBerry App World policy group

Enable Wireless Service Provider Billing IT policy rule

Description	This rule specifies whether a BlackBerry device user can purchase applications from the BlackBerry App World storefront using the purchasing plan for your organization's wireless service provider.
Example	You manage the BlackBerry Enterprise Server Express at a real estate agency. Many of the BlackBerry device users within the agency noticed several applications on the BlackBerry App World storefront that can help them research new properties. You have approval from management to allow employees to purchase the applications using the purchasing plan of the agency's wireless service provider.
Possible values	• Yes • No
Default values	• No
Minimum requirements	• BlackBerry Device Software 4.5
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP2

Bluetooth policy group

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

Disable Bluetooth IT policy rule

Description	This rule specifies whether support for Bluetooth technology on a BlackBerry device is turned off. If Bluetooth technology is turned on when a device receives this rule, the BlackBerry device user must reset the device for the change to take effect.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 3.8
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

Disable Wireless Bypass IT policy rule

Description	This rule specifies whether to prevent wireless bypass using Bluetooth technology on a BlackBerry device.
Example	Many employees have computers with Bluetooth technology. Bluetooth technology allows users to connect their computers to devices that support Bluetooth using a wireless Bluetooth connection. You can allow users to synchronize their devices with the BlackBerry Desktop Software using a Bluetooth connection instead of using the network of your organization's wireless service provider. You can permit Bluetooth connections to help reduce wireless network usage in your organization's environment.
Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry Device Software 4.1

Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP3

Browser policy group

The rules in the Browser policy group apply to all browser configurations on the BlackBerry device.

Disable JavaScript in Browser IT policy rule

Description	This rule specifies whether to permit the execution of JavaScript code on a BlackBerry device.
Example	Some BlackBerry device users report that the BlackBerry Browser is slow when they browse to specific web sites. The web sites might use JavaScript, a scripting language that is used for a wide range of functions including pop-up windows, validating user input, or creating a dynamic interface. You can use this rule to prevent devices from processing JavaScript . This rule disables JavaScript functionality on websites but it might speed up the browsing experience.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP2

MDS Browser Domains IT policy rule

Description	This rule specifies a list of web addresses that a BlackBerry device must retrieve using the BlackBerry Browser and BlackBerry MDS Connection Service. You must separate multiple web addresses with a comma (,). If you want to permit the BlackBerry Browser to retrieve subdomains of a web address, you can prefix the domain with a period (.). For example, you can

	type ".example.com" to permit the BlackBerry Browser to retrieve all subdomains of example.com (such as mail.example.com, www.example.com).
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.2
Rule introduction	• BlackBerry Enterprise Server Express for Microsoft Exchange 5.0 SP2 MR1 • BlackBerry Enterprise Server Express for IBM Lotus Domino 5.0 SP2

Camera policy group

Disable Photo Camera IT policy rule

Description	This rule specifies whether the camera on a BlackBerry device is turned on.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.2
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

Disable Video Camera IT policy rule

Description	This rule specifies whether the video camera on a BlackBerry device is turned on.
Possible values	• Yes

	• No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.3
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

Common policy group

Disable MMS IT policy rule

Description	This rule specifies whether a BlackBerry device user can send and receive MMS messages. For more information, see the *BlackBerry Enterprise Solution Security Technical Overview*.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.0.2
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

Disable Voice Note Recording IT policy rule

Description	This rule specifies whether the Voice Note Recorder application is available on a BlackBerry device.

Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.3
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP2

Email Messaging policy group

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

Confirm External Image Download IT policy rule

Description	This rule specifies whether a BlackBerry device displays a confirmation dialog box when a BlackBerry device user clicks the Get Images link in an HTML-formatted email message. The message that the confirmation dialog box displays informs users that they might expose their email addresses if they download the image from the Internet.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

Disable Manual Download of External Images IT policy rule

Description	This rule specifies whether a BlackBerry device user can manually request to view URL-referenced content (such as pictures) that is embedded in email messages.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.5
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

Disable Notes Native Encryption Forward And Reply IT policy rule

Description	This rule specifies whether to prevent a BlackBerry device user from forwarding and replying to IBM Lotus Domino encrypted email messages using a BlackBerry device. By default, a user that has a device that supports for reading IBM Lotus Domino encrypted email messages can forward and reply to encrypted email messages that were received, decrypted, and decompressed on the device. The BlackBerry Messaging Agent decrypts email messages before the device sends email messages to the recipient as plain text. For more information about reading IBM Lotus Domino encrypted email messages on a device, see the *BlackBerry Enterprise Solution Security Technical Overview*.
Possible values	• Yes • No
Default value	• No

Minimum requirements	• BlackBerry Device Software 4.2.1
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP3

Disable Rich Content Email IT policy rule

Description	This rule specifies whether a BlackBerry device can receive email messages in RTF or HTML format.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.5
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

Maximum Native Attachment MFH attachment size IT policy rule

Description	This rule specifies the maximum size of an attachment that a BlackBerry device user can send from a BlackBerry device. This rule applies to attachments that are larger than 60 KB. If you set this rule to 0, the device cannot send any attachments that are larger than 60 KB. The device can send attachments that are smaller than 60 KB. The device compresses attachments that are smaller than 60 KB and includes the attachments in the body of the email message. If you change the value of the Maximum single attachment upload size (KB) field or the Maximum Upload Attachment Size field to 0, the device cannot upload any attachments that are larger than 60 KB.
Example	Many users send email messages that include large attachments to their coworkers, which can affect the performance of the BlackBerry Enterprise Server Express. You can limit the size of message attachments that users can send from devices to help control network traffic.

Related rules	In BlackBerry Enterprise Server Express 5.0 SP1 or later, this rule interacts with the Maximum single attachment upload size (KB) field in the BlackBerry Administration Service. If you configure this field, the BlackBerry Enterprise Server Express sends the values to the device using service books. The device cannot send an attachment that exceeds the size that you specify in the field.
Possible values	• 0 to 3,145,728 bytes
Default value	• 3,145,728 bytes
Minimum requirements	• BlackBerry Device Software 4.2
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

Maximum Native Attachment MFH total attachment size IT policy rule

Description	This rule specifies the total size of all standard attachments that can be uploaded from a BlackBerry device.
Example	Many BlackBerry device users are sending email messages that include one or more large attachments to their coworkers, which can affect the performance of the BlackBerry Enterprise Server Express. You can limit the total size of message attachments that users can send from devices to help control network traffic.
Possible values	• 0 to 5,242,880 bytes
Default value	• 5,242,880 bytes
Minimum requirements	• BlackBerry Device Software 4.2
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

Maximum Native Attachment MTH attachment size IT policy rule

Description	This rule specifies the maximum size of an attachment that a BlackBerry device user can download to a BlackBerry device. Set this rule to 0 to prevent the user from downloading attachments on the device.
Example	Many BlackBerry device users download message attachments on their devices. The IT staff is concerned about the use of extra network resources and the potential security risk that downloading attachments causes because the sender might not always be a trusted employee. You can prevent users from downloading attachments on their devices. Users can still open and view message attachments.
Possible value	• 0 to 1,048,576 KB
Default value	• 10,240 KB
Minimum requirements	• BlackBerry Device Software 4.5
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

Notes Native Encryption Password Timeout IT policy rule

Description	This rule specifies the maximum length of time that a BlackBerry device stores the IBM Lotus Notes .id password that a BlackBerry device user types. Change this rule to 0 to prevent the device from storing the password that a user types on a device.
Possible values	• -1 to 32,767 minutes
Default value	• -1
Minimum requirements	• BlackBerry Device Software 4.3

Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP3

Require Notes Native Encryption For Outgoing Messages IT policy rule

Description	This rule specifies whether a BlackBerry device user can send email messages that are encrypted using IBM Lotus Notes encryption. If necessary, the BlackBerry device prompts a user for the IBM Lotus Notes encryption passwords. A device does not perform IBM Lotus Notes encryption, it configures email messages that the device sends for IBM Lotus Notes encryption that the BlackBerry Enterprise Server Express performs. This rule does not affect email messages that a device sends using email services that do not support IBM Lotus Notes encryption.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP3

Password policy group

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

Forbidden Passwords IT policy rule

Description	This rule specifies the passwords that a BlackBerry device user cannot use. Separate multiple passwords with a comma (,). By default, a BlackBerry device prevents a user from configuring passwords that use a natural sequence of characters or numbers. The device also automatically prevents common letter substitutions. For example, if you include "password" in the forbidden passwords list, users cannot use "p@ssw0rd", "pa$zword", or "password123" on the device.
Related rules	The Password Required IT policy rule affects this rule. The device uses this rule only if you set the Password Required IT policy rule to Yes.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.1
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

Maximum Password History IT policy rule

Description	This rule specifies the maximum number of previous passwords that a BlackBerry device checks new passwords against to prevent a BlackBerry device user from reusing previous passwords.
Related rules	The Password Required IT policy rule affects this rule. The device uses this rule only if you set the Password Required IT policy rule to Yes.
Example	You notice that many users reuse passwords that they used previously when they are prompted to create a new password for their devices. You want users to create new passwords each time, to reduce the risk of someone discovering a user's password. You set this rule to 15 so that when a user types a new password, it cannot be the same as any of the previous 15 passwords the user specified.
Possible values	• 0 to 15 passwords
Default values	• 0
Minimum requirements	• BlackBerry Device Software 3.6

Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

Periodic Challenge Time IT policy rule

Description	This rule specifies the security timeout interval that must elapse before a BlackBerry device locks and prompts a BlackBerry device user to type a password, regardless of whether the device was active during that interval.
Related rules	The Password Required IT policy rule affects this rule. The device uses this rule only if you set the Password Required IT policy rule to Yes. The User Can Change Timeout IT policy rule affects this rule. Change the User Can Change Timeout IT policy rule to No so that a user cannot change the timeout settings on a device. The Enable Long-Term Timeout IT policy rule affects this rule. By default, if you change the Enable Long-Term Timeout IT policy rule to Yes, the security timeout interval is turned on and set to 60 minutes.
Possible values	• 1 to 1440 minutes
Default value	• 60 minutes
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP2

Set Maximum Password Attempts IT policy rule

Description	This rule specifies the number of times that a BlackBerry device user can try a password before a BlackBerry device permanently deletes all of the application data.
Related rules	The Password Required IT policy rule affects this rule. The device uses this rule only if you set the Password Required IT policy rule to Yes.
Possible values	• 3 to 10
Default value	• 10

Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

Set Password Timeout IT policy rule

Description	This rule specifies the amount of time of inactivity that can occur before a BlackBerry device user must type the password to unlock a BlackBerry device. This rule defines the default value for the security timeout.
Related rules	The User Can Change Timeout IT policy rule affects this rule. If you set the User Can Change Timeout IT policy rule to No, the device uses the security timeout that you set in this rule.
Possible values	• 0 to 60 minutes
Default value	• 2 minutes for BlackBerry Device Software 4.6 and earlier • 30 minutes for BlackBerry Device Software 4.7 and later
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

Suppress Password Echo IT policy rule

Description	This rule specifies whether the characters that a BlackBerry device user types in the Password dialog box appear on the BlackBerry device screen after the user types the password incorrectly a specific number of times.
Related rules	The Password Required IT policy rule affects this rule. The device uses this rule only if a password is configured on the device. To require a password, configure the Password Required IT policy rule to Yes. The Set Maximum Password Attempts IT policy rule affects this rule. To specify the number of times that the user can type the password incorrectly before the characters appear on the screen, configure the Set Maximum Password Attempts IT policy rule.

Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

Personal Devices policy group

Disable Forwarding of Work Content Using Personal Channels IT policy rule

Description	This rule specifies whether a BlackBerry device user can send work data to contacts using personal resources (for example, SMS text messages, MMS messages, or email messages from personal email accounts).
Related rules	The Enable Separation of Work Content IT policy rule affects this rule. A BlackBerry device only uses this rule if you set the Enable Separation of Work Content IT policy rule to Yes.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry 6
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP3

Enable Separation of Work Content IT policy rule

Description	This rule specifies whether a BlackBerry device distinguishes between work data and personal data, and whether only authorized applications on the device can access work data. If you set this rule to Yes and a BlackBerry device user tries to delete a desktop service book, the device prompts the user to delete the work data on the device.
Example	Your organization manages confidential information that cannot be shared with outside sources. All BlackBerry device users in your organization have a custom application on their devices that they use to track and share customer information. You can use this rule and the "Is access to the corporate data API allowed" application control policy rule to give the custom application access to work content and to prevent all other third-party applications on the device from accessing work content such as email messages, contact information, and calendar information.
Related rules	The "Is access to the corporate data API allowed" application control policy rule affects this rule. The "Is access to the corporate data API allowed" application control policy rule specifies whether a third-party application or an add-on application is authorized to access work data. To make this rule affect third-party applications, you must set the "Is access to the corporate data API allowed" application control policy to Disallowed for the third-party application.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry 6
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP3

Require Work Resources for Conducting Work Activities IT policy rule

Description	This rule specifies whether a BlackBerry device must use work resources (for example, work email accounts or work calendars) when a BlackBerry device user conducts work activity (for example, sending an email message to a work contact or scheduling a work appointment).

Related rules	The Enable Separation of Work Content IT policy rule affects this rule. The device only uses this rule if you set the Enable Separation of Work Content IT policy rule to Yes.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry 6
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP3

Work Domains IT policy rule

Description	This rule specifies a list of resources (for example, domain names, server names, and email-address domains) that a BlackBerry device identifies as work resources. If you list a domain, all of the subdomains of the domain are included automatically. If you list multiple resources, separate the resources with a comma (,), semicolon (;), or space. For example, if your organization has multiple domains, type example.com, example.net, example.org. If you set this rule, the device warns a BlackBerry device user when an email message includes an email address that does not belong to a work domain. The device highlights email addresses that do not belong to the work domain in yellow. If the user tries to forward a work email to an email address that does not belong to the work domain or includes an email address that does not belong to the work domain to a reply, the device also displays a warning message.
Default value	• Null value
Minimum requirements	• BlackBerry 6
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP3

PIM Synchronization policy group

Disable All Wireless Synchronization IT policy rule

Description	This rule specifies whether wireless data synchronization is turned off. Set this rule to Yes to turn off all wireless data synchronization, except wireless email reconciliation. This rule prevents the following actions: • Wireless synchronization of contact entries, calendar entries, email filters, tasks, and memos • Wireless synchronization of all logging information • Wireless backup of data, including configuration data for BlackBerry devices • Wireless bulk loads • Activation of devices over the wireless network
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.0

PGP Application policy group

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

PGP Allowed Content Ciphers IT policy rule

Description	This rule specifies the encryption algorithms that a BlackBerry device can use to encrypt PGP protected messages. To maintain compatibility with most PGP clients, use Triple DES encryption and CAST. By default, a device is designed to encrypt email messages using Triple DES encryption if it does not know the decryption capabilities available to a recipient.
Example	Your organization implemented PGP technology to secure email messages and other electronic data that employees send and receive. You install the PGP Support Package for BlackBerry smartphones on devices to allow BlackBerry device users to send and receive PGP email and PIN messages. Your organization supports the use of the AES and Triple DES standards only, so you use this rule to permit devices to use these content ciphers only to encrypt PGP messages.
Possible values	• AES (256-bit) • AES (192-bit) • AES (128-bit) • CAST (128-bit) • Triple DES
Minimum requirements	• PGP Support Package for BlackBerry smartphones 4.1 • BlackBerry Device Software 4.1
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP2

PGP Allowed Encrypted Attachment Mode IT policy rule

Description	This rule specifies the mode for retrieving PGP protected attachment information on a BlackBerry device.
Example	The security standards in your organization specify that users should only open PGP encrypted message attachments on their computers in a highly secure work environment. You can use this rule to prevent users from retrieving PGP encrypted attachments on their devices.

Possible values	• None • Manual • Automatic
Default value	• Automatic
Minimum requirements	• BlackBerry Device Software 4.5
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP2

PGP Allowed Encryption Types IT policy rule

Description	This rule specifies the types of encryption that a BlackBerry device can use for PGP protected messages.
Example	Your organization manages information that demands a high level of security. You can use this rule to support both PGP encryption and conventional encryption for email messages that are sent from and received on devices.
Possible values	• PGP key-based only • Conventional only • Both
Default value	• Both
Minimum requirements	• PGP Support Package for BlackBerry smartphones 4.0 • BlackBerry Device Software 4.6
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP2

PGP Force Digital Signature IT policy rule

Description	This rule specifies whether a BlackBerry device digitally signs all PGP protected messages that it sends. If you apply this rule, you might override email policy settings on the PGP Universal Server.
Example	Your organization implemented PGP technology to secure email messages and other electronic data that employees send and receive. You install the PGP Support Package for BlackBerry smartphones on devices to allow BlackBerry device users to send and receive PGP email and PIN messages. Your organization's security standards require that all email messages must be digitally signed. A digital signature is used to verify that the message was sent from the correct user. You can use this rule to add digital signatures to all PGP messages that are sent from devices.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• PGP Support Package for BlackBerry smartphones 4.1 • BlackBerry Device Software 4.1
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP2

PGP Force Encrypted Messages IT policy rule

Description	This rule specifies whether a BlackBerry device encrypts all PGP protected messages that it sends. If you apply this rule, you might override email policy settings on the PGP Universal Server.
Example	Your organization implemented PGP technology to secure email messages and other electronic data that employees send and receive. You install the PGP Support Package for BlackBerry smartphones on devices to allow BlackBerry device users to send and receive PGP email and PIN messages.

	To meet your organization's requirements for highly secure mobile communication, you can use this rule to make devices encrypt all email messages that users forward or reply to using PGP encryption.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• PGP Support Package for BlackBerry smartphones 4.1 • BlackBerry Device Software 4.1
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP2

PGP Minimum Strong DH Key Length IT policy rule

Description	This rule specifies the minimum Diffie-Hellman key size to use with PGP protected messages.
Example	BlackBerry devices use PGP public keys and PGP private keys to encrypt and decrypt email messages. PGP keys can use the DH algorithm for encryption and decryption. The length of the key in bits is an important factor in determining the strength of the key. Your organization supports a minimum key length of 512 bits for keys that use the DH algorithm, so you specify 512 bits for this rule to permit devices to support PGP keys of this length or greater.
Possible values	• 512 to 4096 bits
Default value	• 1024 bits
Minimum requirements	• PGP Support Package for BlackBerry smartphones 4.1 • BlackBerry Device Software 4.1
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP2

PGP Minimum Strong DSA Key Length IT policy rule

Description	This rule specifies the minimum DSA key size to use with PGP protected messages. The permitted range is 512 through 1024 bits.
Example	BlackBerry devices use PGP public keys and PGP private keys to encrypt and decrypt email messages. PGP keys can use the DSA algorithm for encryption and decryption. The length of the key in bits is an important factor in determining the strength of the key. Your organization supports a minimum key length of 512 bits for keys that use the DSA algorithm, so you specify 512 bits for this rule to permit devices to support PGP keys of this length or greater.
Possible values	• 512 to 1024 bits
Default value	• 1024 bits
Minimum requirements	• PGP Support Package for BlackBerry smartphones 4.1 • BlackBerry Device Software 4.1
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP2

PGP Minimum Strong RSA Key Length IT policy rule

Description	This rule specifies the minimum RSA key size to use with PGP protected messages.
Example	BlackBerry devices use PGP public keys and PGP private keys to encrypt and decrypt email messages. PGP keys can use the RSA algorithm for encryption and decryption. The length of the key in bits is an important factor in determining the strength of the key. Your organization supports a minimum key length of 512 bits for keys that use the RSA algorithm, so you specify 512 bits for this rule to permit devices to support PGP keys of this length or greater.
Possible values	• 512 to 4096 bits
Default value	• 1024 bits
Minimum requirements	• PGP Support Package for BlackBerry smartphones 4.1

	• BlackBerry Device Software 4.1
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP2

PGP More All and Send Mode IT policy rule

Description	This rule specifies the mode that a BlackBerry device uses to retrieve the complete text of an email message when a BlackBerry device user replies to or forwards an email message.
Example	By default, BlackBerry device users must request the complete text of email messages that they reply to or forward as PGP messages from their devices. You can use this rule to make devices automatically retrieve and display the complete text of messages that users reply to or forward as PGP messages.
Possible values	• Automatic • Manual • None
Default value	• Manual
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP2

PGP Universal Enrollment Method IT policy rule

Description	This rule specifies the method that a BlackBerry device user must use to enroll with the PGP Universal Server on a BlackBerry device. The user must submit the enrollment information to the PGP Universal Server before the user sends and receives PGP protected messages on the device.
Example	To support PGP encryption with the PGP Universal Server, BlackBerry device users must enroll their devices with your organization's PGP Universal Server. By default, email-based enrollment is used to enroll devices with the PGP Universal Server. To meet your organization's security

	requirements, you can use this rule to enforce an alternate method that requires users to specify their domain user name and password to enroll their devices.
Possible values	• Domain username/password enrollment • Email-based enrolment
Default value	• Email-based enrollment
Minimum requirements	• PGP Support Package for BlackBerry smartphones 4.1 • BlackBerry Device Software 4.1
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP2

PGP Universal Policy Cache Timeout IT policy rule

Description	This rule specifies the length of time that a BlackBerry device caches the PGP Universal Server address.
Example	BlackBerry devices retrieve the email policy of the PGP Universal Server to determine whether to sign, encrypt, or sign and encrypt email messages. If the email policy does not change often, you can set this rule so that devices retrieve the email policy of the PGP Universal Server every 48 hours.
Possible values	• 4 to 48 hours
Default value	• 24 hours
Minimum requirements	• PGP Support Package for BlackBerry smartphones 4.1 • BlackBerry Device Software 4.1
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP2

PGP Universal Server Address IT policy rule

Description	This rule specifies the address of your organization's PGP Universal Server. The PGP Universal Server applies email policies that the PGP Universal Server administrator configures. Configure this rule to require that the BlackBerry device user registers with the PGP Universal Server. A BlackBerry device that is registered with the PGP Support Package for BlackBerry smartphones enforces compliance with the email policies for all email messages.
Default value	• Null value
Minimum requirements	• PGP Support Package for BlackBerry smartphones 4.1 • BlackBerry Device Software 4.1
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP2

RIM Value-Added Applications policy group

Disable Organizer Data Access for Social Networking Applications IT policy rule

Description	This rule specifies whether a BlackBerry device must prevent social-networking applications from accessing organizer data.
Example	Members of the support staff at a college use Facebook for BlackBerry smartphones to share information about courses, tutoring schedules, and help contacts. You can allow social-networking applications to access calendar information and contact information on devices so that the support staff can share the information with students using the application.
Possible values	• Yes • No

Default value	• Yes
Minimum requirements	• BlackBerry Device Software 4.2.0
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP3

Security policy group

Allow External Connections IT policy rule

Description	This rule specifies whether applications, including third-party applications, can initiate external connections (for example, to WAP gateways).
Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP2

Allow Resetting of Idle Timer IT policy rule

Description	This rule specifies whether a BlackBerry device permits third-party applications to reconfigure the inactivity-timeout value on the device and bypass the timeout value for the device password. For more information about the inactivity timeout, visit www.blackberry.com/go/apiref to read the EventInjector class and Backlight.enable() method in the API reference for the BlackBerry Java Development Environment.

Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.2.1
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP2

Allow Split-Pipe Connections IT policy rule

Description	This rule specifies whether applications, including third-party applications, can open internal and external connections on a BlackBerry device at the same time. An application may create a security issue if it opens internal and external connections at the same time because the application can collect data from inside the firewall and send it outside the firewall.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP2

Allow Third Party Apps to Use Serial Port IT policy rule

Description	This rule specifies whether third-party applications can use the serial port, IrDA port, or USB port on a BlackBerry device.
Example	BlackBerry device users in your organization use a custom application that allows them to upload customer data onto their computers that they collect during off-site visits. The application requires the use of the USB port on devices to connect to computers. You can use this rule to permit the application to use the USB port on devices.

Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP2

Content Protection Strength IT policy rule

Description	This rule specifies the cryptographic strength that a BlackBerry device uses for content protection of data that it receives when it is locked. When you specify a value for this rule, content protection is turned on. If you set this rule to Strong, the device uses a 160-bit ECC public key. If you set this rule to Stronger, the device uses a 283-bit ECC public key. If you set this rule to Strongest, the device uses a 571-bit ECC public key. For devices that are running BlackBerry Device Software 5.0 and later with onboard device memory, this rule also encrypts the onboard device memory using the BlackBerry device user password and a device-generated key. Media files in the onboard device memory are not encrypted unless you set the Encryption on On-Board Device Memory Media Files IT policy rule. For devices that are running BlackBerry Device Software 4.7 and earlier, you can configure the External File System Encryption Level IT policy rule to encrypt media files on the media card.
Related rules	The Password Required IT policy rule affects this rule. A device uses this rule only if you set the Password Required IT policy rule to Yes. This rule affects the Minimum Password Length IT policy rule. If you set this rule to Stronger, you should set the Minimum Password Length IT policy rule to 12 characters. If you set this rule to Strongest, you should set the Minimum Password Length IT policy rule to 21 characters.
Possible values	• Strong • Stronger • Strongest
Default values	• Null value

Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

Disable 3DES Transport Crypto IT policy rule

Description	This rule specifies whether to prevent a BlackBerry device from using the Triple DES algorithm to encrypt and decrypt data.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP2

Disable External Memory IT policy rule

Description	This rule specifies whether to prevent a BlackBerry device user from accessing the media card on a BlackBerry device.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.2
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

Disable GPS IT policy rule

Description	This rule specifies whether the GPS feature on a BlackBerry device is turned on. If you set this rule to Yes, BlackBerry Maps does not work and applications cannot access the GPS APIs for the device.
Related rules	This rule affects the "Is Access to the GPS API Allowed" application control policy rule setting. This rule overrides the "Is Access to the GPS API Allowed" application control policy rule setting.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.3
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP2

Disable IP Modem IT policy rule

Description	This rule specifies whether the IP modem on a BlackBerry device is available.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

Disable USB Mass Storage IT policy rule

Description	This rule specifies whether USB mass storage and the media transport protocol are turned on. The media transport protocol permits a BlackBerry device user to transfer media files from a computer or BlackBerry Desktop Manager to a BlackBerry device or media card. When you transfer files using the media transport protocol, the device does not protect the files using content protection and does not encrypt the data on the media card, even if you configure the External File System Encryption Level IT policy rule. This feature is not available for BlackBerry Desktop Manager 4.2.2 because the Roxio Media Manager uses the media transport protocol to transfer files. For more information about protecting data that a device stores on a media card, see the *BlackBerry Enterprise Solution Security Technical Overview*.
Possible values	• Yes • No
Default values	• Yes in the Default IT policy.
Minimum requirements	• BlackBerry Device Software 4.2
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP2

Disallow Third Party Application Downloads IT policy rule

Description	This rule specifies whether a BlackBerry device user can install or update applications on a BlackBerry device using the BlackBerry Browser or BlackBerry App World. If you set this rule to Yes, the user cannot install or update applications on the device using BlackBerry Browser or BlackBerry App World. The user can install or update an application that Research In Motion creates using the BlackBerry Desktop Software. This rule does not apply to RIM Add-on applications in software configurations. If you set this rule to Yes, the BlackBerry Administration Service prevents you from using a software configuration to install third-party applications that are digitally signed with code

	signing keys on the device. After you apply this rule, any signed third-party applications are removed from the device and the user cannot reinstall them.
Related rules	This rule affects the Application Restriction Rule IT policy rule. If you set this rule to Yes, it takes precedence over the Application Restriction Rule IT policy rule. This rule affects the Category Restriction Rule IT policy rule. If you set this rule to Yes, it takes precedence over the Category Restriction Rule IT policy rule. This rule is affected by the Application Installation Methods IT policy rule. If you disallow specific application methods using the Application Installation Methods rule, the Application Installation Methods rule takes precedence on BlackBerry 7.1 and higher devices.
Possible values	• Yes • No
Default values	• No in the Default IT policy
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

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

Description	This rule specifies whether the media files that are located in the on-board memory of a BlackBerry device are encrypted to the BlackBerry device user password and the device-generated key.
Related rules	The Content Protection Strength IT policy rule affects this rule. The device uses this rule only if you configure the Content Protection Strength IT policy rule.
Possible values	• Allowed • Required • Disallowed
Default value	• Allowed

Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

External File System Encryption Level IT policy rule

Description	This rule specifies the level of encryption that a BlackBerry device uses to encrypt files that it stores on a media card. You can use this rule to require that the device encrypts a media card, either including or excluding media-card files. You cannot use this rule to encrypt files that a BlackBerry device user transfers to the media card manually (for example, from a USB mass storage device). The master keys for the media card are stored on the media card. A device is designed to use the master keys to decrypt and encrypt files on the media card. A device is designed to use the device key, a user-provided password, or both to encrypt the master keys.
Possible values	• Encrypt to User Password (excluding multimedia directories) • Encrypt to User Password (including multimedia directories) • Encrypt to Device Key (excluding multimedia directories) • Encrypt to Device Key (including multimedia directories) • Encrypt to User Password and Device Key (excluding multimedia directories) • Encrypt to User Password and Device Key (including multimedia directories) • Not required
Default values	• Not required
Minimum requirements	• BlackBerry Device Software 4.2
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

Force Lock When Holstered IT policy rule

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

Possible values	• Yes • No
Default values	• No in the Default IT policy
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

Required Password Pattern IT policy rule

Description	This rule specifies the required pattern for a BlackBerry device password. A character in the password pattern specifies the character type permitted in its position in the password. Passwords can contain Latin-1 characters only. If you configure this rule, a BlackBerry device user can only create a password that is greater than or equal to the length of the pattern on the device. Password characters that exceed the pattern length can be letters, numbers, or symbols. You can use the following characters to specify the password pattern: • 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
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.2

Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP2

Reset to Factory Defaults on Wipe IT policy rule

Description	This rule specifies whether a BlackBerry device resets to the factory default settings when it receives the Delete all device data and disable device IT administration command over the wireless network. For devices that are running BlackBerry Device Software 5.0 and later, this rule is enforced both remotely (when an administrator erases the data on a device remotely) and locally (for example, when a BlackBerry device user exceeds the maximum number of times that the user can try to type the password or erases all data on the device). For devices that are running BlackBerry Device Software 4.7 and earlier, this rule is enforced only when an administrator erases the data remotely.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.2.2
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP2

Security Transcoder Cod File Hashes IT policy rule

Description	This rule specifies the hashes for the .cod files of a transcoder that a BlackBerry device needs to register the transcoder. Set each hash in hexadecimal format and separate multiple values with a comma (,).
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.5

Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP3

S/MIME Application policy group

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

Entrust Messaging Server (EMS) Email Address IT policy rule

Description	This rule specifies the email address for your organization's Entrust Entelligence Messaging Server.
Example	Your organization uses an Entrust Entelligence Messaging Server to secure email messages that employees send. You can use this rule to allow BlackBerry devices to communicate with the EMS and support EMS functionality that integrates with devices.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.0 • S/MIME Support Package for BlackBerry smartphones 4.0
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP2

S/MIME Allowed Content Ciphers IT policy rule

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

Example	You install the S/MIME Support Package for BlackBerry smartphones on devices to allow users to send and receive S/MIME signed and S/MIME signed and encrypted email and PIN messages. Your organization supports the use of AES and Triple DES only, so you use this rule to permit devices to use these content ciphers only to encrypt S/MIME messages.
Possible values	• AES (256-bit) • AES (192-bit) • AES (128-bit) • CAST (128-bit) • RC2 (128-bit) • Triple DES • RC2 (64-bit) • RC2 (40-bit)
Default value	• AES (256-bit), AES (192-bit), AES (128-bit), CAST (128-bit), RC2 (128-bit), and Triple DES
Minimum requirements	• BlackBerry Device Software 3.6 • S/MIME Support Package for BlackBerry smartphones 1.5
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

S/MIME Allowed Encrypted Attachment Mode IT policy rule

Description	This rule specifies the mode for retrieving S/MIME-protected attachment information on a BlackBerry device.
Example	The security standards in your organization specify that BlackBerry device users should open S/MIME-encrypted message attachments on their computers in a highly secure work environment only. You can use this rule to prevent users from retrieving S/MIME-encrypted attachments on their devices.
Possible values	• Automatic • Manual

	• None
Default value	• Automatic
Minimum requirements	• BlackBerry Device Software 4.5
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP2

S/MIME Allowed Encryption Types IT policy rule

Description	This rule specifies the types of encryption that a BlackBerry device can use with S/MIME-protected email messaging.
Example	Some users in your organization are planning a confidential project and want to maintain the security of their email messages. You install the S/MIME Support Package for BlackBerry smartphones on devices to allow BlackBerry device users to send and receive S/MIME signed and S/MIME signed and encrypted email and PIN messages. You can configure this IT policy rule so that the users must use a shared password to encrypt and decrypt email messages.
Possible values	• Certificate-based encryption • Password-based encryption • Both
Default value	• Both
Minimum requirements	• BlackBerry Device Software 4.6 • S/MIME Support Package for BlackBerry smartphones 4.0
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP2

S/MIME Force Digital Signature IT policy rule

Description	This rule specifies whether a BlackBerry device sends all S/MIME-protected email messages with a digital signature.

Example	You install the S/MIME Support Package for BlackBerry smartphones on devices to allow users to send and receive S/MIME signed and S/MIME signed and encrypted email and PIN messages. Your organization's security standards require that all email messages must be digitally signed. A digital signature is used to verify that an email message was sent from the correct user. You can use this rule to add digital signatures to all S/MIME messages that users send from devices.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 3.6 • S/MIME Support Package for BlackBerry smartphones 1.5
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP2

S/MIME Force Encrypted Messages IT policy rule

Description	This rule specifies whether a BlackBerry device encrypts all email messages that a BlackBerry device user sends using S/MIME encryption.
Example	You install the S/MIME Support Package for BlackBerry smartphones on devices to allow users to send and receive S/MIME signed and S/MIME signed and encrypted email and PIN messages. To meet your organization's requirements for highly secure mobile communication, you can use this rule to make devices encrypt all email messages that users forward or reply to using S/MIME encryption.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 3.6 • S/MIME Support Package for BlackBerry smartphones 1.5

Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

S/MIME Minimum Strong DH Key Length IT policy rule

Description	This rule specifies the minimum Diffie-Hellman key size to use with S/MIME-protected email messages.
Example	BlackBerry devices use S/MIME public keys and S/MIME private keys to encrypt and decrypt email messages. S/MIME keys can use the DH algorithm for encryption and decryption. The length of the key in bits is a factor in determining the strength of the key. Your organization supports a minimum key length of 512 bits for keys that use the DH algorithm, so you specify 512 bits for this rule to permit devices to support S/MIME keys of this length or greater.
Possible values	• 512 to 4096 bits
Default value	• 1024 bits
Minimum requirements	• BlackBerry Device Software 3.6 • S/MIME Support Package for BlackBerry smartphones 1.5
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP2

S/MIME Minimum Strong DSA Key Length IT policy rule

Description	This rule specifies the minimum DSA key size that a BlackBerry device uses with S/MIME-protected email messages.
Example	BlackBerry devices use S/MIME public keys and S/MIME private keys to encrypt and decrypt email messages. S/MIME keys can use the DSA algorithm for encryption and decryption. The length of the key in bits is a factor in determining the strength of the key. Your organization supports a minimum key length of 512 bits for keys that use the DSA algorithm, so you specify 512 bits for this rule to permit devices to support S/MIME keys of this length or greater.
Possible values	• 512 to 1024 bits

Default value	• 1024 bits
Minimum requirements	• BlackBerry Device Software 3.6 • S/MIME Support Package for BlackBerry smartphones 1.5
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP2

S/MIME Minimum Strong ECC Key Length IT policy rule

Description	This rule specifies the minimum ECC key size that a BlackBerry device uses with S/MIME-protected email messages.
Example	BlackBerry devices use S/MIME public keys and S/MIME private keys to encrypt and decrypt email messages. S/MIME keys can use the ECC algorithm for encryption and decryption. The length of the key in bits is a factor in determining the strength of the key. Your organization supports a minimum key length of 160 bits for keys that use the ECC algorithm, so you specify 160 bits for this rule to permit devices to support S/MIME keys of this length or greater.
Possible values	• 163 to 571 bits
Default value	• 163 bits
Minimum requirements	• BlackBerry Device Software 3.6 • S/MIME Support Package for BlackBerry smartphones 1.5
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP2

S/MIME Minimum Strong RSA Key Length IT policy rule

Description	This rule specifies the minimum RSA key size that a BlackBerry device uses with S/MIME-protected email messages.

Example	BlackBerry devices use S/MIME public keys and S/MIME private keys to encrypt and decrypt email messages. S/MIME keys can use the RSA algorithm for encryption and decryption. The length of the key in bits is a factor in determining the strength of the key. Your organization supports a minimum key length of 512 bits for keys that use the RSA algorithm, so you specify 512 bits for this rule to permit devices to support S/MIME keys of this length or greater.
Possible values	• 512 to 4096 bits
Default value	• 1024 bits
Minimum requirements	• BlackBerry Device Software 3.6 • S/MIME Support Package for BlackBerry smartphones 1.5
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP2

S/MIME More All and Send Mode IT policy rule

Description	This rule specifies the mode that a BlackBerry device uses to retrieve the complete text of an email message if a BlackBerry device user replies to or forwards the email message.
Example	By default, BlackBerry device users must request the complete text of email messages that they reply to or forward as S/MIME messages from their devices. You can use this rule to make devices automatically retrieve and display the complete text of email messages that users reply to or forward as S/MIME messages.
Possible values	• Automatic • Manual • None
Default value	• Manual
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP2

VPN policy group

VPN User Name IT policy rule

Description	This rule specifies the default user name that a BlackBerry device uses to log in to your organization's VPN server. Specify a value for this rule if you want to configure a default user name for all user accounts. If a BlackBerry device user types a user name on a device manually, IT policy updates overwrite or delete the value that the user typed. To retain the value on the device, verify that the updated rule uses the same value as this rule.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

VPN User Password IT policy rule

Description	This rule specifies the default password that a BlackBerry device uses to log in to your organization's VPN server. Specify a value for this rule if you want to configure a default password for all user accounts. If a BlackBerry device user types a password on a device manually, IT policy updates overwrite or delete the value that the user typed. To retain the value on the device, verify that the updated rule uses the same value as this rule.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

Wi-Fi policy group

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

Disable Wi-Fi IT policy rule

Description	This rule specifies whether a BlackBerry device user can access a Wi-Fi network from a Wi-Fi enabled BlackBerry device.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.2.1
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

Wired Software Updates policy group

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

Allow Web-Based Software Loading IT policy rule

Description	This rule specifies whether a BlackBerry device user can update the BlackBerry Device Software using software loading feature over the Internet.
Example	Your organization has a small IT staff. You want employees to be able to update the BlackBerry Device Software on their devices without having to request an update from the IT department.

	You can use this rule to allow users to update the BlackBerry Device Software using the BlackBerry Device Software Update web site (www.blackberry.com/update).
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

Cryptographic Services Backup IT policy rule

Description	This rule specifies whether a BlackBerry device can back up cryptographic services data when a BlackBerry device user updates the BlackBerry Device Software. A cryptographic service is any service that uses a cryptographic key to protect communication on the device. If you allow the device to back up cryptographic services data, the device can continue to use a cryptographic service after the software loading process completes without requiring the user to reactivate the device manually.
Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

Wireless Software Upgrades policy group

Disallow Patch Download Over Roaming WAN IT policy rule

Description	This rule specifies whether to prevent a BlackBerry device from downloading updates for the BlackBerry Device Software over a WAN connection when roaming.
Example	You do not want BlackBerry device users to upgrade the BlackBerry Device Software over the wireless network using a roaming WAN connection, because this connection type does not meet your organization's security requirements and network usage standards. You can use this rule to prevent users from updating the BlackBerry Device Software using a roaming WAN connection.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.5
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

Configuration settings

5

Configuration settings for Wi-Fi profiles

Associated Certificate Authority Configuration configuration setting

Description	This setting specifies the name of the certificate authority profile in the Certificate Authority Profile Name IT policy rule. The certificate authority profile consists of credentials that a BlackBerry device can use to initiate a certificate-enrollment process. After you associate a certificate authority profile with a Wi-Fi profile, you can assign the Wi-Fi profile to a user account and send the profile to the device.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 5.0

Associated VPN Profile configuration setting

Description	This setting specifies the name of the VPN profile that you want to associate with the Wi-Fi profile.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.2.0

Wi-Fi Allow AP to AP Handover configuration setting

Description	This setting specifies whether a BlackBerry device can perform Wi-Fi handovers between wireless access points.
Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry Device Software 4.2.1

Wi-Fi Allow Handheld Changes configuration setting

Description	This setting specifies whether a BlackBerry device user can change the Wi-Fi policy settings on a BlackBerry device.
Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry Device Software 4.0

Wi-Fi Allow Password Save configuration setting

Description	This setting specifies whether a BlackBerry device user can save passwords for authentication to a Wi-Fi network on a BlackBerry device.
Possible values	• Yes • No

Default value	• Yes
Minimum requirements	• BlackBerry Device Software 4.2.1

Wi-Fi Band Type configuration setting

Description	This setting specifies the band types that you configure the wireless access points of a specific SSID to operate on.
Possible values	• 802.11 a/b/g • 802.11 b/g • 802.11 a • 802.11 b
Default value	• 802.11 a/b/g
Minimum requirements	• BlackBerry Device Software 4.2.2

Wi-Fi BlackBerry Infrastructure Wi-Fi Access Mode configuration setting

Description	This setting specifies whether a BlackBerry device can connect to the BlackBerry Infrastructure over a Wi-Fi network.
Related settings	This configuration setting affects the BlackBerry Infrastructure Wi-Fi Access Mode IT policy rule. When you change this setting, you override the BlackBerry Infrastructure Wi-Fi Access Mode IT policy rule. You can use this configuration setting to configure the access mode for a specific Wi-Fi network, and the IT policy rule to configure the access mode for other Wi-Fi networks. The BlackBerry Infrastructure Wi-Fi Access Mode IT policy rule affects this configuration setting. If you turn off access to the BlackBerry Infrastructure over a Wi-Fi network using the BlackBerry Infrastructure Wi-Fi Access Mode IT policy rule, you cannot override the IT policy rule using this configuration setting.

Possible values	• Access does not require VPN • Access requires VPN • Access disabled
Default value	• Access does not require VPN
Minimum requirements	• BlackBerry Device Software 5.0

Wi-Fi Default Gateway configuration setting

Description	This setting specifies the default gateway in IP address format (for example, 10.0.0.1) that a BlackBerry device can use if DHCP on the device is turned off.
Related settings	The Wi-Fi DHCP Configuration configuration setting affects this configuration setting. The device uses this configuration setting only if you change the Wi-Fi DHCP Configuration configuration setting to No.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.2

Wi-Fi Default Key ID configuration setting

Description	This setting specifies the default WEP key ID. Verify that the WEP key ID matches the WEP access point ID and the corresponding WEP key.
Possible values	• 1 to 4
Default value	• 1
Minimum requirements	• BlackBerry Device Software 4.0

Wi-Fi DHCP Configuration configuration setting

Description	This setting specifies whether your organization uses DHCP for dynamic network configuration. If your organization uses a Wi-Fi network that includes subnets, turn on DHCP to permit roaming between subnets.
Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry Device Software 4.2

Wi-Fi Disable Server Certificate Validation configuration setting

Description	This setting specifies whether a BlackBerry device requires a certificate authority certificate for server authentication when it uses a PEAP, EAP-TLS, or EAP-TTLS authentication method to connect to a Wi-Fi network. If you change this setting to Yes, a root certificate is not required for the PEAP, EAP-TLS, or EAP-TTLS authentication method.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 5.0

Wi-Fi Domain Suffix configuration setting

Description	This setting specifies the suffix for the internal domain name in FQDN format.
Related settings	The Wi-Fi DHCP Configuration configuration setting affects this configuration setting. Configure this setting only if you change the Wi-Fi DHCP Configuration configuration setting to No to make DHCP unavailable.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.2.1

Wi-Fi EAP-FAST Provisioning method configuration setting

Description	This setting specifies the type of provisioning method that a BlackBerry device can use when it authenticates with a Wi-Fi network using EAP-FAST authentication with PAC. If you want the server to authenticate the device using the user name and password for the user account and a root certificate when the device connects for the first time, you can select the Authenticated option. The device does not connect to the server if the server does not provide a root certificate to the device. If you want the server to authenticate the device using the user name and password for the user account without server authentication, you can select the Anonymous option. If you want the server to authenticate the device using the user name and password for the user account, and you want the settings on the server to determine if server authentication must occur, you can select the Both option. If the server provides a root certificate, the device verifies the server using the selected root certificate. If the server does not present a root certificate, the device does not perform server authentication.
Possible values	• Anonymous • Authenticated • Both
Default value	• Anonymous

Minimum requirements	• BlackBerry Device Software 5.0

Wi-Fi Enable Authentication Page configuration setting

Description	This setting specifies whether the Wi-Fi Login browser is available on a BlackBerry device. Change this setting to Yes to permit a BlackBerry device user to log in to a captive portal using the device.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.0

Wi-Fi Hard Token Required configuration setting

Description	This setting specifies whether a BlackBerry device requires a hard token for authentication. Change this setting to Yes if the device requires a hard token (for example, RSA SecurID) as part of the password for authentication.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.2.1

Wi-Fi Inner Authentication Mode configuration setting

Description	This setting specifies the authentication mode that a BlackBerry device uses for tunneled EAP security.
Possible values	• None • EAP-MSCHAPV2 • EAP-GTC • PAP • CHAP • MSCHAP • MSCHAPV2 • EAP-MD5
Default value	• None
Minimum requirements	• BlackBerry Device Software 4.2.1

Wi-Fi Internet Access Path configuration setting

Description	This setting specifies how a BlackBerry device must access the Internet for Wi-Fi profiles that you configure for your organization.
Possible values	• Access through Wi-Fi • Access through BlackBerry MDS Connection Service • Auto-select
Default value	• Auto-select
Minimum requirements	• BlackBerry 6

Wi-Fi IP Address configuration setting

Description	This setting specifies the IP address (for example, 10.0.0.1) that a BlackBerry device can use if DHCP on the device is turned off.
Related settings	The Wi-Fi DHCP Configuration configuration setting affects this configuration setting. The device uses this setting only if you change the Wi-Fi DHCP Configuration configuration setting to No.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.2

Wi-Fi Link Security configuration setting

Description	This setting specifies the authentication method that a BlackBerry device requires to access a Wi-Fi network.
Possible values	• Open Wi-Fi security • WEP • PSK • EAP-PEAP • EAP-LEAP • ESP-TLS • EAP-FAST • EAP-TTLS • EAP-SIM • EAP-AKA
Default value	• Open Wi-Fi security
Minimum requirements	• BlackBerry Device Software 4.0

Wi-Fi Minimal EAP-TLS Certificate Encryption Key Security Level configuration setting

Description	This setting specifies the minimum security level for a private key that an EAP authentication method uses with a client certificate. If you configure this setting to Medium security, a BlackBerry device prompts a BlackBerry device user only once for the key store password so that the device can retrieve the private key and encrypt email messages. After the device retrieves the private key, the device retrieves the private key again only after the user resets the device. The device caches the private key in memory but does not store it with the Wi-Fi profile. If you configure this setting to High security, the device always prompts the user for the key store password when it accesses the private key and encrypts email messages. The device does not store the unencrypted private key with the Wi-Fi profile. If you configure this setting to Low security, the device prompts the user only once for the key store password so that the device can retrieve the private key and encrypt email messages. The device stores the unencrypted private key with the Wi-Fi profile.
Possible values	• Low security • High security • Medium security
Default value	• Low security
Minimum requirements	• BlackBerry Device Software 4.0

Wi-Fi Preshared Key configuration setting

Description	This setting specifies the PSK if you use PSK in your organization to authenticate to Wi-Fi networks.
Related settings	The Wi-Fi Link Security configuration setting affects this configuration setting. A BlackBerry device uses this setting only if you set the Wi-Fi Link Security configuration setting to PSK.
Default value	• Null value

Minimum requirements	• BlackBerry Device Software 4.0

Wi-Fi Primary DNS configuration setting

Description	This setting specifies the primary DNS in IP address format (for example, 10.0.0.1) that a BlackBerry device can use if DHCP on the device is turned off.
Related settings	The Wi-Fi DHCP Configuration configuration setting affects this configuration setting. The device uses this configuration setting only if you change the Wi-Fi DHCP Configuration configuration setting to No.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.2

Wi-Fi Profile Editability configuration setting

Description	This setting specifies whether a BlackBerry device user can change the settings in the Wi-Fi profile on a BlackBerry device. If you change this setting to No editability, the user cannot change any settings in the Wi-Fi profile. If you change this setting to Credentials editability, the user can change only the user credentials in the Wi-Fi profile.
Possible values	• Full editability • No editability • Credentials editability
Default value	• Full editability
Minimum requirements	• BlackBerry Device Software 4.2.1

Wi-Fi Profile Visibility configuration setting

Description	This setting specifies whether a BlackBerry device user can view the settings in the Wi-Fi profile. If you configure this setting to Restricted visibility, the BlackBerry device displays only the profile name. When you configure this setting to Credentials visibility, the device displays only the profile name and login information for the user.
Possible values	• Full visibility • Restricted visibility • Credentials visibility
Default value	• Full visibility
Minimum requirements	• BlackBerry Device Software 4.2.1

Wi-Fi Roaming Threshold configuration setting

Description	This setting determines how often the Wi-Fi transceiver of a BlackBerry device scans for nearby wireless access points and roams to one of the access points if the signal quality is better than the signal of the current access point. If you configure this setting to Low, the device roams only when signal quality is very low. If you configure this setting to Medium, the device roams when the signal quality is medium to low. If you configure this setting to High, the device roams aggressively to access points with better signal strength. If you configure this setting to Auto, the device selects roaming thresholds automatically.
Possible values	• Auto • Low • Medium • High
Default value	• Auto

Minimum requirements	• BlackBerry Device Software 4.2.1

Wi-Fi Secondary DNS configuration setting

Description	This setting specifies the secondary DNS in IP address format (for example, 10.0.0.1) that a BlackBerry device can use if DHCP on the device is turned off.
Related settings	The Wi-Fi DHCP Configuration configuration setting affects this rule. A device uses this setting only if you change the Wi-Fi DHCP Configuration configuration setting to No.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.2

Wi-Fi Server SAN configuration setting

Description	This setting specifies a SAN field for the server certificate. If you do not specify a SAN field for the server certificate, a BlackBerry device accepts any valid server certificate.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.2.1

Wi-Fi Server Subject configuration setting

Description	This setting specifies the Subject field for the server certificate. If you do not specify the Subject field for a server certificate, a BlackBerry device accepts any valid server certificate.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.2.1

Wi-Fi SSID configuration setting

Description	This setting specifies the network name of a Wi-Fi network and its wireless access points. The SSID is case-sensitive and limited to 32 characters.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.0

Wi-Fi Subnet Mask configuration setting

Description	This setting specifies the subnet mask in IP address format (for example, 10.0.0.1) that a BlackBerry device can use if DHCP on the device is turned off.
Related settings	The Wi-Fi DHCP Configuration configuration setting affects this rule. The device uses this setting only if you change the Wi-Fi DHCP Configuration configuration setting to No.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.2

Wi-Fi Token Serial Number configuration setting

Description	If a BlackBerry device requires that a software token is part of the password for authentication, this setting specifies the serial number of the software token that is provided to the device.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.2.1

Wi-Fi User Name configuration setting

Description	This setting specifies the user name for PEAP authentication or LEAP authentication on a BlackBerry device. Configure this setting if you want to create a default value for all BlackBerry device users. If the user types a user name on the device manually, IT policy updates overwrite or delete the value that the user types. To retain the user-specified value on the device, verify that the updated Wi-Fi profile uses the same value as the Wi-Fi profile on the device.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.0

Wi-Fi User Password configuration setting

Description	This setting specifies the password for PEAP authentication or LEAP authentication on a BlackBerry device. Configure this setting if you want to create a default value for all BlackBerry device users. If the user types a password on the device manually, IT policy updates overwrite or delete the value that the user types. To retain the user-specified value on the device, verify that the updated Wi-Fi profile uses the same value as the Wi-Fi profile on the device.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.2

Wi-Fi WEP Key 1 configuration setting

Description	This setting specifies the password for WEP key 1 using the format *xx:xx:xx:xx:xx*. This configuration setting supports 5 or 13 pairs of hexadecimal digits (0 to 9 and A to F) that you separate with a colon (:). For example, AB:CD:EF:01:23 or AB:CD:EF:01:23:45:67:89:AB:CD:EF:01:23.
Default value	• Null value

Minimum requirements	• BlackBerry Device Software 4.0

Wi-Fi WEP Key 2 configuration setting

Description	This setting specifies the password for WEP key 2 using the format *xx:xx:xx:xx:xx*. This configuration setting supports 5 or 13 pairs of hexadecimal digits (0 to 9 and A to F) that you separate with a colon (:). For example, AB:CD:EF:01:23 or AB:CD:EF:01:23:45:67:89:AB:CD:EF:01:23.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.0

Wi-Fi WEP Key 3 configuration setting

Description	This setting specifies the password for WEP key 3 using the format *xx:xx:xx:xx:xx*. This configuration setting supports 5 or 13 pairs of hexadecimal digits (0 to 9 and A to F) that you separate with a colon (:). For example, AB:CD:EF:01:23 or AB:CD:EF:01:23:45:67:89:AB:CD:EF:01:23.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.0

Wi-Fi WEP Key 4 configuration setting

Description	This setting specifies the password for WEP key 4 using the format *xx:xx:xx:xx:xx*. This configuration setting supports 5 or 13 pairs of hexadecimal digits (0 to 9 and A to F) that you separate with a colon (:). For example, AB:CD:EF:01:23 or AB:CD:EF:01:23:45:67:89:AB:CD:EF:01:23.
Default value	• Null value

Minimum requirements	• BlackBerry Device Software 4.0

Configuration settings for VPN profiles

Associated Certificate Authority Configuration configuration setting

Description	This setting specifies the name of the certificate authority profile in the Certificate Authority Profile Name IT policy rule. The certificate authority profile consists of credentials that a BlackBerry device can use to initiate a certificate-enrollment process. After you associate a certificate authority profile with a VPN profile, you can assign the VPN profile to a user account and send the profile to the device.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 5.0 • BlackBerry Enterprise Server Express 5.0 SP4

Enable VPN configuration setting

Description	This setting specifies whether the VPN client on a BlackBerry device is turned on. If you change this setting to Yes, the device must use a VPN server to access a Wi-Fi network. If you change this setting to No, the device might not be able to use a Wi-Fi network that requires VPN access, or it might require the use of an alternative form of access control.
Possible values	• Yes • No
Default value	• No

Minimum requirements	• BlackBerry Device Software 4.2

Split-tunneling Mode configuration setting

Description	This setting specifies whether a BlackBerry device can use split-tunneling to bypass an active VPN connection.
Possible values	• Enable on all networks • Disable on corporate networks • Disable on all networks
Default value	• Disable on all networks
Minimum requirements	• BlackBerry Device Software 5.0

Suppress VPN Banner configuration setting

Description	This setting specifies whether the VPN dialog box displays on a BlackBerry device after the device connects to a VPN server.
Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry Device Software 4.2.1

Use VPN Xauth configuration setting

Description	This setting specifies whether the VPN client on a BlackBerry device should use Xauth certificates to authenticate with your organization's VPN gateway.

Related settings	The Enable VPN configuration setting affects this configuration setting. You must change the Enable VPN configuration setting to Yes so that the device can use this configuration setting.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.2

VPN Allow Handheld Changes configuration setting

Description	This setting specifies whether a BlackBerry device user can change all of the VPN policy rules on a BlackBerry device. If you change this setting to No, a user can continue to change the VPN user name and VPN password on the device.
Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry Device Software 4.0

VPN Allow Password Save configuration setting

Description	This setting specifies whether a BlackBerry device user can save the VPN password on a BlackBerry device.
Possible values	• Yes • No
Default value	• Yes

Minimum requirements	• BlackBerry Device Software 4.2

VPN Disable Server Certificate Validation configuration setting

Description	This setting specifies whether a BlackBerry device requires a certificate to authenticate with VPN gateways that support PKI-based authentication using certificates. This setting applies to the following VPN gateways that support PKI-based authentication using certificates: the Cisco Secure PIX Firewall, Cisco IOS with Easy VPN Server, NetScreen Series Security Systems, and Nortel Networks Contivity VPN switch.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 5.0

VPN DNS Configuration configuration setting

Description	This setting specifies your organization's VPN DNS configuration. To require that a BlackBerry device retrieves DNS settings from the VPN gateway, change this setting to Yes. To require that the device uses the static settings that are specified in the VPN Primary DNS configuration setting, VPN Secondary DNS configuration setting, and VPN Domain Name configuration setting, change this setting to No.
Related settings	The Enable VPN configuration setting affects this configuration setting. You must set the Enable VPN configuration setting to Yes so that the device uses this configuration setting.
Possible values	• Yes • No
Default setting	• Yes

Minimum requirements	• BlackBerry Device Software 4.2

VPN Domain Name configuration setting

Description	This setting specifies the suffix for your organization's domain name using the FQDN format.
Related settings	The Enable VPN configuration setting affects this configuration setting. You must set the Enable VPN configuration setting to Yes so that a BlackBerry device uses this configuration setting. The VPN DNS Configuration configuration setting affects this configuration setting. You must set the VPN DNS Configuration configuration setting to No so that the device uses this configuration setting.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.2

VPN Gateway Address configuration setting

Description	This setting specifies the IP address or FQDN of your organization's VPN server.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.2

VPN Group Name configuration setting

Description	This setting specifies the group name of your organization's VPN server. Specify the group name for your organization's VPN server only if the VPN client requires it.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.2

VPN Group Password configuration setting

Description	This setting specifies the group password for your organization's VPN server. Specify the group password for your organization's VPN server only if the VPN client requires it.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.2

VPN Hard Token Required configuration setting

Description	This setting specifies whether the VPN server requires that a BlackBerry device uses a hard token as part of the password for authentication.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.2.1

VPN IKE Cipher configuration setting

Description	This setting specifies the encryption algorithm that a BlackBerry device uses to authenticate IKE exchanges. Change this setting only if the encryption algorithm does not support AES128.
Possible values	• DES • 3DES • AES128 • AES192 • AES256

Default value	• AES128
Minimum requirements	• BlackBerry Device Software 4.2

VPN IKE DH Group configuration setting

Description	This setting specifies the DH group that a BlackBerry device uses to generate key material. Change this setting only if the the DH group does not use ECC.
Related settings	The Enable VPN configuration setting affects this rule. You must change the Enable VPN configuration setting to Yes so that the device can use this setting.
Possible values	• Group 1 • Group 2 • Group 5 • Group 7 • Group 9
Default value	• Group 7
Minimum requirements	• BlackBerry Device Software 4.2

VPN IKE Hash configuration setting

Description	This setting specifies the hash method authentication code that a BlackBerry device can use. Change this setting only if the hash method authentication code does not support SHA1 160 bits.
Possible values	• MD5 128 bits • SHA1 160 bits
Default value	• SHA1 160 bits

Minimum requirements	• BlackBerry Device Software 4.2

VPN IP Address configuration setting

Description	This setting specifies the IP address of the VPN.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.2.1

VPN IPSec Cipher and Hash configuration setting

Description	This setting specifies the encryption algorithm and hash that a BlackBerry device uses for IPSec Security Associations. Change this setting only if the IPSec Hash and Cipher are not SHA1 Hash and AES128 Cipher.
Possible values	• MD5 Hash with No Cipher • SHA1 Hash with No Cipher • No Hash with DES Cipher • MD5 Hash and DES Cipher • SHA1 Hash and DES Cipher • No Hash and 3DES Cipher • MD5 Hash and 3DES Cipher • SHA1 Hash and 3DES Cipher • No Hash and AES128 Cipher • MD5 Hash and AES128 Cipher • SHA1 Hash and AES128 Cipher • No Hash and AES192 Cipher • MD5 Hash and AES192 Cipher • SHA1 Hash and AES192 Cipher • No Hash and AES256 Cipher

	• MD5 Hash and AES256 Cipher • SHA1 Hash and AES256 Cipher
Default value	• SHA1 Hash and AES128 Cipher
Minimum requirements	• BlackBerry Device Software 4.2

VPN Minimal Certificate Encryption Key Security Level configuration setting

Description	This setting specifies the minimum security level for private keys that a BlackBerry device uses for authentication methods that require client certificates. If you change this setting to High security, the device always prompts a BlackBerry device user for the key store password when the device requires access to the private key. This might happen frequently, even if the user types the password recently. Private keys are not stored with the VPN profile. If you change this setting to Medium security, the device prompts the user for the key store password the first time and then prompts the user only after the user resets the device. Private keys are cached in memory but are not stored with the VPN profile. If you change this setting to Low security, A device prompts the user for the key store password only once. The device retrieves and stores the private key in unencrypted format with the VPN profile.
Possible values	• Low security • High security • Medium security
Default value	• Low security
Minimum requirements	• BlackBerry Device Software 4.2.1

VPN NAT Keep Alive configuration setting

Description	This setting specifies the NAT keep-alive frequency. Specify the interval that a BlackBerry device sends a keep-alive packet to the VPN concentrator to maintain the connection to the VPN concentrator.
Possible values	• 1 to 1439 minutes
Default value	• 1 minute
Minimum requirements	• BlackBerry Device Software 4.2

VPN PFS configuration setting

Description	This setting specifies whether PFS is turned on for a BlackBerry device. Change this setting only if your organization does not support PFS.
Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry Device Software 4.2

VPN Primary DNS configuration setting

Description	This setting specifies the static setting for the IP address of your organization's primary DNS server.
Related settings	The Enable VPN configuration setting affects this configuration setting. You must change the Enable VPN configuration setting to Yes so that a BlackBerry device can use this configuration setting.

	The VPN DNS Configuration configuration setting affects this configuration setting. You must change the VPN DNS Configuration configuration setting to No so that the device can use this configuration setting.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.2

VPN Profile Visibility configuration setting

Description	This setting specifies whether a BlackBerry device user can view the configuration settings of the VPN profile on a BlackBerry device.
Possible values	• Full visibility • Restricted visibility • Credentials visibility
Default value	• Full visibility
Minimum requirements	• BlackBerry Device Software 4.2.1

VPN Profile Editability configuration setting

Description	This setting specifies whether a BlackBerry device user can change the configuration settings of the VPN profile on a BlackBerry device.
Possible values	• Full editability • No editability • Credentials editability
Default value	• Full editability
Minimum requirements	• BlackBerry Device Software 4.2.1

VPN Secondary DNS configuration setting

Description	This setting specifies the static setting for the IP address of your organization's secondary DNS server.
Related settings	The Enable VPN configuration setting affects this configuration setting. You must change the Enable VPN configuration setting to Yes so that a BlackBerry device can use this setting. The VPN DNS Configuration configuration setting affects this configuration setting. You must change the VPN DNS Configuration configuration setting to No so that the device can use this setting.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.2

VPN Subnet 1 IP Address configuration setting

Description	This setting specifies the IP address of subnet 1 for VPN gateways that require a BlackBerry device to specify a subnet. Type the IP address in dot-decimal notation (for example, 192.0.2.1).
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.6

VPN Subnet 1 Mask configuration setting

Description	This setting specifies the subnet mask of subnet 1 for VPN gateways that require a BlackBerry device to specify a subnet.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.6

VPN Subnet 2 IP Address configuration setting

Description	This setting specifies the IP address of subnet 2 for VPN gateways that require a BlackBerry device to specify a subnet. Type the IP address in dot-decimal notation (for example, 192.0.2.1).
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.6

VPN Subnet 2 Mask configuration setting

Description	This setting specifies the subnet mask of subnet 2 for VPN gateways that require a BlackBerry device to specify a subnet.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.6

VPN Subnet 3 IP Address configuration setting

Description	This setting specifies the IP address of subnet 3 for VPN gateways that require a BlackBerry device to specify a subnet. Type the IP address in dot-decimal notation (for example, 192.0.2.1).
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.6

VPN Subnet 3 Mask configuration setting

Description	This setting specifies the subnet mask of subnet 3 for VPN gateways that require a BlackBerry device to specify a subnet.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.6

VPN Subnet Mask configuration setting

Description	This setting specifies the IP address of the subnet mask of the VPN.
Related settings	This configuration setting affects the Enable VPN configuration setting. If you change this configuration setting, you must set the Enable VPN configuration setting to Yes. This configuration setting affects the VPN DNS Configuration configuration setting. If you change this configuration setting, you must set the VPN DNS Configuration configuration setting to No.
Default setting	• Null value
Minimum requirements	• BlackBerry Device Software 4.2.1

VPN Token Serial Number configuration setting

Description	If the VPN server requires that a BlackBerry device uses a software token as part of the password for authentication, this setting specifies the serial number of the software token that is provisioned for the device.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.2.1

VPN User Name configuration setting

Description	This setting specifies the default user name that a BlackBerry device uses to log in to your organization's VPN server. Configure this setting if you want to create a default user name for all user accounts. If a BlackBerry device user types a user name on the device manually, IT policy updates overwrite or delete the value that the user typed. To retain the value that the user types on the device, verify that the updated configuration setting uses the same value as this setting.
Related settings	The Enable VPN configuration setting affects this configuration setting. You must change the Enable VPN configuration setting to Yes so that the device can use this setting.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.2

VPN User Password configuration setting

Description	This setting specifies the default password that a BlackBerry device uses to log in to your organization's VPN server. Configure this setting if you want to create a default password for all user accounts. If a BlackBerry device user types a password on the device manually, IT policy updates overwrite or delete the value that the user typed. To retain the value that the user types on the device, verify that the updated configuration setting uses the same value as this configuration setting.
Related settings	The Enable VPN configuration setting affects this configuration setting. You must change the Enable VPN configuration setting to Yes so that the device can use this configuration setting.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.2

VPN Vendor Type configuration setting

Description	This setting specifies the type of VPN client that the VPN client on a BlackBerry device emulates.
Related settings	The Enable VPN configuration setting affects this configuration setting. You must set the Enable VPN configuration setting to Yes so that the device can use this configuration setting.
Possible values	• Alcatel 7130 Secure VPN Gateway Family • Avaya VSU(TM) Series • Check Point(TM) Software Technologies VPN-1 • Cisco VPN Concentrator 3000 Series • Cisco Secure PIX Firewall VPN • Cisco IOS with Easy VPN Server • Cosine IPX VPN Gateway • Cylink Nethawk • Intel®) Netstructure(TM) 3100 Series • Lucent Firewall Brick Family • Netscreen Systems • Nortel Networks Contivity VPN Switch Series • ReefEdge Connect Server • Secure Computing Sidewinder(TM) Firewall • Symantec Raptor Firewall and PowerVPN
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.2

VPN Xauth Type configuration setting

Description	This setting specifies the type of authentication that BlackBerry device users must use for your organization's VPN server.

Related settings	The Enable VPN configuration setting affects this configuration setting. You must change the Enable VPN configuration setting to Yes so that a BlackBerry device can use this configuration setting.
Possible values	• User name and password required • SecurID required
Default value	• User name and password required
Minimum requirements	• BlackBerry Device Software 4.2

Application control policy rules 6

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

Are External Network Connections Allowed application control policy rule

Description	This rule specifies whether an application can make external network connections. You can configure this rule to prevent the application from sending or receiving any data on a BlackBerry device using an external protocol (such as WAP or TCP). You can also configure this rule so that an application prompts a BlackBerry device user before it makes external connections through the device firewall.
Related rules	The List of External Domains application control policy rule affects this rule. The List of External Domains application control policy rule takes precedence over this application control policy rule.
Possible values	• Not permitted • Allowed • Prompt user
Default value	• Prompt user
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

Are Internal Network Connections Allowed application control policy rule

Description	This rule specifies whether an application can make internal network connections. You can configure this rule to prevent the application from sending or receiving any data on a BlackBerry device using an internal protocol (for example, the BlackBerry MDS Connection Service). You can also configure this rule so that an application prompts a BlackBerry device user before it makes internal connections through the device firewall.
Related rules	The List of Internal Domains application control policy rule affects this rule. The List of Internal Domains application control policy rule takes precedence over this application control policy rule.
Possible values	• Not permitted • Allowed • Prompt user
Default value	• Prompt user
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

Are Local Connections Allowed application control policy rule

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

Possible values	• Disallowed • Allowed
Default value	• Allowed
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

Can Device Settings be Modified application control policy rule

Description	This rule specifies whether an application can change configuration settings and BlackBerry device user settings on a BlackBerry device.
Possible values	• Not permitted • Allowed • Prompt user
Default value	• Allowed
Minimum requirements	• BlackBerry Device Software 4.2.1
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

Can the Security Timer be Reset application control policy rule

Description	This rule specifies whether an application can reset the amount of time that must elapse before a BlackBerry device locks automatically.
Possible values	• Not permitted • Allowed • Prompt user
Default value	• Not permitted
Minimum requirements	• BlackBerry Device Software 4.2.1
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

Display information while locked application control policy rule

Description	This rule specifies whether an application can display information on a BlackBerry device screen when the device is locked.
Possible values	• Not permitted • Allowed • Prompt user
Default value	• Not permitted

Minimum requirements	• BlackBerry 6
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP3

Disposition application control policy rule

Description	This rule specifies whether an application is optional, required, or not permitted on the BlackBerry device. You can use this rule to make a specific application required on the device or to prevent unspecified or untrusted applications from being installed on the device.
Possible values	• Optional • Required • Not permitted
Default value	• Optional
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

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

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

Default value	• Disallowed
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

Is Access to the Corporate Data Allowed application control policy rule

Description	This rule specifies whether a third-party application or an add-on application developed by Research In Motion can access work data on a BlackBerry device. You can configure this rule to prevent third-party applications or add-on applications developed by RIM from accessing work data on the device. The device checks this rule to determine which applications can access work data.
Possible values	• Disallowed • Allowed
Default value	• Allowed
Minimum requirements	• BlackBerry 6
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP3

Is Access to the Email API Allowed application control policy rule

Description	This rule specifies whether an application can send and receive email messages using a BlackBerry device.
Possible values	• Disallowed • Allowed
Default value	• Allowed
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

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

Description	This rule specifies whether an application can simulate input events on a BlackBerry device, such as pressing keys or performing trackball actions.
Possible values	• Disallowed • Allowed
Default value	• Allowed
Minimum requirements	• BlackBerry Device Software 4.0

Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

Is Access to the File API Allowed application control policy rule

Description	This rule specifies whether an application can access, change, delete, and move files on a BlackBerry device.
Possible values	• Disallowed • Allowed
Default value	• Allowed
Minimum requirements	• BlackBerry Device Software 4.2
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

Is Access to the GPS API Allowed application control policy rule

Description	This rule specifies whether an application can access the GPS APIs on a BlackBerry device. You can configure this rule to prevent the application from accessing the GPS APIs on a device or to prompt the BlackBerry device user before an application can access the GPS APIs.
Possible values	• Not permitted • Allowed • Prompt user

Default value	• Prompt user
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

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

Description	This rule specifies whether an application can access the key store APIs on a BlackBerry device.
Possible values	• Disallowed • Allowed
Default value	• Allowed
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

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

Description	This rule specifies whether an application can perform cross-application communication operations. You can use this rule to permit two or more applications to share data or for one application to use the connection permissions of another application.
Possible values	• Disallowed • Allowed
Default value	• Allowed
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

Is Access to the Media API Allowed application control policy rule

Description	This rule specifies whether an application can run or create multimedia files on a BlackBerry device.
Possible values	• Disallowed • Allowed
Default value	• Allowed

Minimum requirements	• BlackBerry Device Software 4.3
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

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

Description	This rule specifies whether an application can add, change, or delete Java .cod files on a BlackBerry device.
Possible values	• Disallowed • Allowed
Default value	• Allowed
Minimum requirements	• BlackBerry Device Software 4.3
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

Is Access to the Near Field Communication (NFC) Allowed application control policy rule

Description	This rule specifies whether an application can access NFC on a BlackBerry device.
Possible values	• Not permitted

	• Allowed • Prompt user
Default value	• Allowed
Minimum requirements	• BlackBerry 7
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP4

Is Access to the PIM API Allowed application control policy rule

Description	This rule specifies whether an application can access the BlackBerry device PIM APIs, which control access to a BlackBerry device user's personal information, such as contacts, on a device. If you permit an application to access PIM data APIs and use network connection protocols, the application might be able to send all of the user's personal information from the device.
Possible values	• Disallowed • Allowed
Default value	• Allowed
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

Is Access to the Phone API Allowed application control policy rule

Description	This rule specifies whether an application can make calls, answer incoming calls, and access call logs on a BlackBerry device. You can configure this rule to prevent an application from making calls on a device or to prompt a BlackBerry device user to permit calls before the application makes calls.
Possible values	• Not permitted • Allowed • Prompt user
Default value	• Prompt user
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

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

Description	This rule specifies whether an application can record media, such as audio and video, using the BlackBerry Browser or other applications on a BlackBerry device.
Possible values	• Not permitted • Allowed

	• Prompt user
Default value	• Not permitted
Minimum requirements	• BlackBerry Device Software 4.2.1
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

Is Access to the Secure Element Allowed application control policy rule

Description	This rule specifies whether an application can access the Secure Element on a BlackBerry device.
Possible values	• Not permitted • Allowed • Prompt user
Default value	• Allowed
Minimum requirements	• BlackBerry 7
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP4

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

Description	This rule specifies whether an application can access the Bluetooth SPP API.
Possible values	• Disallowed • Allowed
Default value	• Allowed
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

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

Description	This rule specifies whether an application can access the user authenticator framework API. The user authenticator framework permits the registration of drivers that provide two-factor authentication to unlock a BlackBerry device. This rule applies to the BlackBerry Device Software and third-party Java applications. For devices that are running BlackBerry Device Software 5.0 and later, this rule applies to drivers for smart card readers and to custom two-factor authentication methods that are created by developers in your organization. For devices that are running BlackBerry Device Software 4.7 and earlier, this rule applies to drivers for smart cards only.

Possible values	• Disallowed • Allowed
Default value	• Allowed
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

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

Description	This rule specifies whether an application on a BlackBerry device can send and receive data over a Wi-Fi connection and access information about the Wi-Fi network.
Possible values	• Not permitted • Allowed • Prompt user
Default value	• Prompt user
Minimum requirements	• BlackBerry Device Software 4.2.1
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

Is Key Store Medium Security Allowed application control policy rule

Description	This rule specifies whether an application can access key-store items that are stored at the medium security level. The application must prompt a BlackBerry device user for the key-store password when it tries to access the private key for the first time or when the private key password timeout expires.
Possible values	• Disallowed • Allowed
Default value	• Allowed
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

Is manage connections allowed application control policy rule

Description	This rule specifies whether an application can manage connections and connection-related information on a BlackBerry device.
Possible values	• Disallowed • Allowed
Default value	• Allowed

Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP3

Is media control allowed application control policy rule

Description	This rule specifies whether an application can open or manage media files on a BlackBerry device.
Possible values	• Not permitted • Allowed • Prompt user
Default value	• Allowed
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP3

Is Theme Data Allowed application control policy rule

Description	This rule specifies whether a BlackBerry device user can use custom theme applications that are developed using the Plazmic Content Developer's Kit as themes on a BlackBerry device.
Possible values	• Disallowed • Allowed
Default value	• Allowed

Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

List of Browser Filter Domains application control policy rule

Description	This rule specifies the list of domains that an application can apply browser filters to web-page content to on a BlackBerry device. For example, you can specify www.google.com and www.yahoo.com as domains for which an application can use a browser filter for search engines.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

List of External Domains application control policy rule

Description	This rule specifies the external domain names that an application can connect to. This rule does not support wildcard characters. You must separate different domains with a semi-colon (;). You can configure this application control policy rule and a pull rule that the BlackBerry MDS Connection Service uses to control whether a BlackBerry device user can access an external domain. If you configure this rule and a pull rule for an external domain, the user cannot access the external domain unless this rule and the pull rule permit access.
Related rules	This rule affects the Are External Network Connections Allowed application control policy rule. The application on a BlackBerry device can connect to domains that you specify in this rule even

	if you set the Are External Network Connections Allowed application control policy rule to Not permitted.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

List of Internal Domains application control policy rule

Description	This rule specifies the internal domain names that an application can establish a connection to. This rule does not support wildcard characters. You must separate different domains with a semi-colon (;).
Related rules	This rule affects the Are Internal Network Connections Allowed application control policy rule. The application on a BlackBerry device can connect to the domains that you specify in this rule even if you set the Are Internal Network Connections Allowed application control policy rule to Not permitted.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server Express 5.0 SP1

Examples of security goals

7

Requiring the use of a password on a device

Scenario	IT policy rule	IT policy group	Value
Extend your organization's password policy to BlackBerry devices.	Password Required	Device only policy group	Yes
	Maximum Password Age	Device only policy group	30
	Minimum Password Length	Device only policy group	8
	Password Pattern Checks	Device only policy group	At least 1 alpha, 1 numeric, and 1 special character
	Set Password Timeout	Password policy group	5
	User Can Change Timeout	Device only policy group	No
Delete all user data on the device if a BlackBerry device user types the password incorrectly.	Set Maximum Password Attempts	Password policy group	10
Do not permit a user to reuse an expired password.	Maximum Password History	Password policy group	10

Preventing the unauthorized use of a device

Scenario	IT policy rule	Policy group	Value
Lock the BlackBerry device automatically, regardless of user activity.	Enable Long-Term Timeout	Device only policy group	Yes
Require that a BlackBerry device user types the password periodically.	Periodic Challenge Time	Password policy group	60
Lock the device automatically after a period of user inactivity.	Maximum Security Timeout	Device only policy group	10

Encrypting data on a device

Scenario	IT policy rule	Policy group	Value
Protect BlackBerry device user and application data on the BlackBerry device.	Content Protection Strength	Security	Strongest
Specify the algorithms that the device uses to encrypt and decrypt PGP messages.	PGP Allowed Content Ciphers	PGP Application	AES (256-bit), AES (192-bit), AES (128-bit), and Triple DES
Specify the algorithms that the device uses to encrypt and decrypt S/MIME messages.	S/MIME Allowed Content Ciphers	S/MIME Application	AES (256-bit), AES (192-bit), AES (128-bit), and Triple DES

Restricting messaging on a device

Scenario	IT policy rule	Policy group	Value
Restrict messaging on a BlackBerry device to messaging	Allow Other Browser Services	Service Exclusivity	No

Scenario	IT policy rule	Policy group	Value
services that your organization can monitor.	Allow Other Message Services	Service Exclusivity	No
	Allow Peer-to-Peer Messages	Device only	No
	Allow SMS	Device only	No
	Disable Forwarding Between Services	Security	Yes
	Disable Cut/Copy/ Paste	Security	Yes
Require a BlackBerry device user to send encrypted email messages from the device.	S/MIME Force Encrypted Messages	S/MIME Application	Yes
	PGP Force Encrypted Messages	PGP Application	Yes
Prevent the user from sending PIN messages.	Allow Peer-to-Peer Messages	Device only	No
Prevent the user from sending SMS text messages.	Allow SMS	Device only	No
Prevent the user from forwarding or replying to email messages using a different messaging service.	Disable Forwarding Between Services	Security	Yes

Defining measures to prevent threats from viruses and malicious users

Consider using IT policy rules and application control policy rules to block threats from viruses and other methods of attack by users with malicious intent.

Limiting the resources that a third-party application can access on a device

Scenario	Example application control policy rule	Value
Prevent third-party Java applications from accessing a list of domains using the BlackBerry Browser.	List of Browser Filter Domains	addresses of the domains
Permit a third-party Java application from sending and receiving messages on a BlackBerry device.	Is Access to the Email API Allowed	Allowed
Remove a third-party Java application from BlackBerry devices over the wireless network.	Disposition	Disallowed
Permit a third-party Java application to access the phone application on BlackBerry devices.	Is Access to the Phone API Allowed	Allowed
Permit a third-party Java application to create public external network connections and permit connections to external domains without prompting users for a password on their BlackBerry devices.	Are External Network Connections Allowed	Allowed
	List of External Domains	addresses of the external domains
Permit a third-party Java application to establish connections to Bluetooth enabled devices.	Is Access to the Serial Port Profile for Bluetooth API Allowed	Allowed
	Are External Network Connections Allowed	Allowed
Prevent users from turning on a custom theme that was created using the Plazmic Content Developer's Kit.	Is Theme Data Allowed	Disallowed
Prevent users from unlocking their BlackBerry devices using a BlackBerry Smart Card Reader and an authentication password.	Is Access to the User Authenticator API Allowed	Disallowed

Limiting user control of third-party applications on BlackBerry devices

Scenario	Example policy rule	Value
Prevent third-party applications from accessing serial ports or USB ports on BlackBerry devices.	Allow Third Party Apps to Use Serial Port (IT policy rule)	No
Prevent users from downloading third-party applications or themes to their BlackBerry devices.	Disallow Third Party Application Downloads (IT policy rule)	Yes
Prevent users from removing a third-party Java application installed on their BlackBerry devices.	Disposition (application control policy rule)	Required
Prevent users from installing a third-party Java application on their BlackBerry devices.	Disposition (application control policy rule)	Disallowed
Remove a third-party Java application from BlackBerry devices over the wireless network.	Disposition (application control policy rule)	Disallowed
Prevent users from turning on a custom theme that was created using the BlackBerry Theme Studio.	Is Theme Data Allowed (application control policy rule)	Required
Prevent users from unlocking their BlackBerry devices using a BlackBerry Smart Card Reader and an authentication password.	Is Access to the User Authenticator API allowed (application control policy rule)	Required
Prevent users that are authenticating through a VPN connection from using third-party applications on their BlackBerry devices.	Is Access to the User Authenticator API allowed (application control policy rule)	Required

Preventing RIM value-added applications from running on BlackBerry devices

You can use application control policy rules and IT policy rules to control whether Research In Motion value-added applications are available on BlackBerry devices. RIM value-added applications include the BlackBerry Wallet and the ecommerce content optimization engine for the BlackBerry Browser.

To prevent the RIM value-added applications from running on BlackBerry Device Software versions earlier than 4.5, you can block all RIM value-added applications using the Disable RIM Value-Added Applications IT policy rule, or you can block specific RIM value-added applications using application-specific IT policy rules.

To prevent the RIM value-added applications from running on BlackBerry Device Software version 4.5 or later, you can use any of the following application-specific methods:

Application	Method
BlackBerry Wallet	• Configure the Disable BlackBerry Wallet IT policy rule to Yes. • Apply an application control policy rule to block all third-party applications, or apply an application control policy to block specific RIM value-added applications if you want to remove the RIM value-added applications from BlackBerry devices. • Configure the Disable RIM Value-Added Applications IT policy rule to Yes.
ecommerce content optimization engine for the BlackBerry Browser	• Configure the Disable Ecommerce Content Optimization Engine IT policy rule to Yes. • Apply an application control policy rule to block all third-party applications, or apply an application control policy to block specific RIM value-added applications if you want to remove the RIM value-added applications from BlackBerry devices. • Configure the Disable RIM Value-Added Applications IT policy rule to Yes.

You can apply the Disposition application control policy rule to RIM value-added applications only. Other application control policy rules do not apply to RIM value-added applications.

Glossary

8

AES	Advanced Encryption Standard
API	application programming interface
BIP	Bearer Independent Protocol
CAST	Computer Assisted Seriation Test
DES	Data Encryption Standard
DH	Diffie-Hellman
DSA	Digital Signature Algorithm
EAP-LEAP	Extensible Authentication Protocol Lightweight Extensible Authentication Protocol
ECC	Elliptic Curve Cryptography
FTP	File Transfer Protocol
gateway message envelope	The gateway message envelope protocol is a Research In Motion proprietary protocol that allows the transfer of compressed and encrypted data between the wireless network and BlackBerry devices. The protocol defines a routing layer that specifies the types of message contents allowed and the addressing information for the data. Gateways and routing components use this information to identify the type and source of the BlackBerry device data, and the appropriate destination service to route the data to.
GPS	Global Positioning System
HTML	Hypertext Markup Language
IP	Internet Protocol
IT	information technology
MFH	message from handheld
MMS	Multimedia Messaging Service
MTH	message to handheld
NFC	Near Field Communication
PIM	personal information management
PIN	personal identification number

RC	Rivest's Cipher
S/MIME	Secure Multipurpose Internet Mail Extensions
SMS	Short Message Service
SPP	Serial Port Profile
TCP	Transmission Control Protocol
USB	Universal Serial Bus
VPN	virtual private network
WAN	wide area network
WAP	Wireless Application Protocol
xAuth	Extended Authentication

Legal notice

9

EXCLUDED AS SET OUT ABOVE, BUT CAN BE LIMITED, ARE HEREBY LIMITED TO NINETY (90) DAYS FROM THE DATE YOU FIRST ACQUIRED THE DOCUMENTATION OR THE ITEM THAT IS THE SUBJECT OF THE CLAIM.

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

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

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

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

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

agreements applicable thereto with third parties, except to the extent expressly covered by a license or other agreement with RIM.

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

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

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

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

Published in Canada