Policy Reference Guide

BlackBerry Enterprise Server

Version: 5.0
Service Pack: 4

Published: 2015-01-14
SWD-20150114144050886

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

New in this release

2

New IT policy rules

Policy group	Rule	BlackBerry Device Software minimum requirement
BlackBerry App World	Public Channel Downloads	5.0
BlackBerry Bridge	Enable BlackBerry Bridge	5.0
BlackBerry Bridge	Private Transport	5.0
BlackBerry Bridge	Public Transport	5.0
BlackBerry Messenger	BBM Voice	5.0
Bluetooth	Human Interface Device Profile	5.0
Browser	Disable Pre-IETF WebSocket Connections in Browser	7.0
Browser	IETF WebSocket Connections in Browser	7.1
Browser	SecureKey Browser Plug-in	7.1
Common	Disable FM Radio	7.1
Companion Devices	BlackBerry PlayBook Log Submission	5.0
Device Configuration	CCL Data Collection	4.0
Documents To Go	Disable Creating and Editing Files Using Documents To Go	7.0
Instant Messaging	Disable BBM-Connected App Features	5.0
Media Server	Media Server	7.1
NFC	Allow NFC Card Emulation Mode	7.0

Policy group	Rule	BlackBerry Device Software minimum requirement
NFC	Allow NFC Peer to Peer Device Communication Mode	7.0
NFC	Allow NFC Tag Reader/Writer	7.0
NFC	NFC Features	7.0
On-Device Diagnostics	Application Resource Monitor	7.1
On-Device Diagnostics	Battery Saving Mode	7.1
Phone	Enable Auto-Answer Incoming Call User Option	7.0
Phone	Disable Enhanced Caller ID Information Lookup	7.1
RIM Value-Added Applications	Disable BlackBerry Radio	6.0
RIM Value-Added Applications	Plans Application	4.5
Secure Email	Suggest Default Encoding for All Outgoing Email and PIN Messages	7.0
Security	Allow Synchronization of Data From Voice Enabled Search	7.0
Security	Allow Voice Enabled Search	7.0
Security	Application Installation from Specific URLs Only	7.1
Security	Application Installation Methods	7.1
Security	Force Cryptographic Power Analysis Protection	7.0
Security	Lock Button Usage	5.0
Security	Primary Transcoder	7.1
Security	Use Camera When Locked	7.1
Security	Use Media Controls When Locked	7.1
Wi-Fi	Allow Mobile Hotspot Mode	7.1
Wi-Fi	Disable Data Exchange for Mobile Hotspot Mode	7.1

Policy group	Rule	BlackBerry Device Software minimum requirement
Wi-Fi	Disable Enterprise Wi-Fi Profiles Backup	7.0
Wi-Fi	Override Hotspot APN Information	7.1
Wi-Fi	Prohibited SSIDs for Mobile Hotspot Mode	7.0

For information about adding IT policy rules to a BlackBerry Enterprise Server from an IT policy pack, search the BlackBerry Technical Solution Center at www.blackberry.com/support for the knowledge base article that includes the IT policy pack.

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 Administration Guide*.

Preconfigured IT policies

The BlackBerry Enterprise Server includes the following preconfigured IT policies that you can change to create IT policies that meet the requirements of your organization.

Preconfigured IT policy	Description
Default	This policy includes all the standard IT policy rules that are set on the BlackBerry Enterprise Server.
Individual-Liable Devices	Similar to the Default IT policy, this policy prevents BlackBerry device users from accessing organizer data from within the social networking applications on their BlackBerry devices. This policy permits users to access their personal calendar services and email messaging services (for example, their BlackBerry Internet Service accounts), update the BlackBerry Device Software using methods that exist outside your organization, make calls when devices are locked, and cut, copy, and paste text. Users cannot forward email messages from one email messaging service to another. You can use the Individual-Liable Devices IT policy if your organization includes users who purchase their own devices and connect the devices to a BlackBerry Enterprise Server instance in your organization's environment.
Basic Password Security	Similar to the Default IT policy, this policy also requires a basic password that users can use to unlock their devices. Users must change the passwords regularly. The IT policy includes a password timeout that locks devices.

Preconfigured IT policy	Description
Medium Password Security	Similar to the Default IT policy, this policy also requires a complex password that users can use to unlock their devices. Users must change the passwords regularly. This policy includes a maximum password history and turns off Bluetooth technology on devices.
Medium Security with No 3rd Party Applications	Similar to the Medium Password Security, this policy requires a complex password that a user must change frequently, a security timeout, and a maximum password history. This policy prevents users from making their devices discoverable by other Bluetooth enabled devices and prevents devices from downloading third-party applications.
Advanced Security	Similar to the Default IT policy, this IT policy also requires a complex password that users must change frequently, a password timeout that locks devices, and a maximum password history. This policy restricts Bluetooth technology on devices, turns on strong content protection, turns off USB mass storage, and requires devices to encrypt external file systems.
Advanced Security with No 3rd Party Applications	Similar to the Advanced Security IT policy, this IT policy requires a complex password that users must change frequently, a password timeout that locks devices, and a maximum password history. This policy restricts Bluetooth technology on devices, turns on strong content protection, turns off USB mass storage, requires devices to encrypt external file systems, and prevents devices from downloading third-party applications.

IT policy rules

4

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

Application Center policy group

Disable Application Center IT policy rule

Description	This rule specifies whether to prevent the application center from running on a BlackBerry device.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.3
Rule introduction	• BlackBerry Enterprise Server 4.1 SP6 • KB16396

Disable Carrier Directory IT policy rule

Description	This rule specifies whether to prevent a BlackBerry device user from accessing the wireless service provider directory in the application center on a BlackBerry device.
Possible values	• Yes

	• No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.3
Rule introduction	• BlackBerry Enterprise Server 4.1 SP6 • KB16396

BlackBerry App World policy group

Application Restriction Rule IT policy rule

Description	This rule specifies whether a BlackBerry device user can purchase and download the applications from the BlackBerry App World storefront that you list in the Application Restriction List IT policy rule. If you set this rule to None, the user can purchase and download all of the applications available from BlackBerry App World.
Related rules	The Disallow Third Party Application Downloads IT policy rule affects this rule. If you set the Disallow Third Party Application Downloads IT policy rule to Yes, it takes precedence over this rule. The Application Restriction List IT policy rule affects this rule. You specify the application that this rule applies to in the Application Restriction List IT policy rule.
Possible values	• Allow • Deny • None
Default value	• None
Minimum requirements	• BlackBerry Device Software 4.5

Rule introduction	• BlackBerry Enterprise Server 5.0 SP2

Application Restriction List IT policy rule

Description	This rule specifies the application IDs of applications on the BlackBerry App World storefront that you can permit or prevent a BlackBerry device user from purchasing and downloading. You must separate multiple application IDs in the list using commas (,). To find the application ID for an application, visit http://appworld.blackberry.com/webstore and browse to the application in BlackBerry App World. The application ID is the number that is displayed in the URL at the top of the browser.
Related rules	This rule affects the Application Restriction Rule IT policy rule. You must configure the Application Restriction Rule IT policy rule to indicate whether a user can purchase and download the applications from BlackBerry App World that you specify in this rule.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.5
Rule introduction	• BlackBerry Enterprise Server 5.0 SP2

Category Restriction Rule IT policy rule

Description	This rule specifies whether a BlackBerry device user can purchase and download applications from the categories on the BlackBerry App World storefront that you specify in the Category Restriction List IT policy rule. If you set this rule to None, the user can purchase and download applications from all of the categories available from BlackBerry App World.
Related rules	The Disallow Third Party Application Downloads IT policy rule affects this rule. If you set the Disallow Third Party Application Downloads IT policy rule to Yes, it takes precedence over this rule. The Category Restriction List IT policy rule affects this rule. You specify the categories that this rule applies to in the Category Restriction List IT policy rule.
Possible values	• Allow

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

Category Restriction List IT policy rule

Description	This rule specifies a list of application categories on the BlackBerry App World storefront that you can permit or prevent a BlackBerry device user from purchasing and downloading. The list displays each category by the category ID. You must separate multiple category IDs in the list using commas (,). For example, if you want to prevent a user from purchasing and downloading applications from the Entertainment, Games, and Shopping categories, type 7, 1, 45. To find the category ID for an application category, visit http://appworld.blackberry.com/webstore and click the application category. The category ID is the number that is located at the end of the URL for the application category.
Related rules	This rule affects the Category Restriction Rule IT policy rule. You must configure the Category Restriction Rule IT policy rule to indicate whether a user can purchase and download the applications from BlackBerry App World that are in the categories that you specify in this rule.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.5
Rule introduction	• BlackBerry Enterprise Server 5.0 SP2

Disable App World IT policy rule

Description	This rule specifies whether the BlackBerry App World storefront is available on a BlackBerry device.

Related rules	This rule takes precedence over the Disable BlackBerry App World IT policy rule in the Security policy group. In BlackBerry Enterprise Server 5.0 SP2 and later and BlackBerry App World 2.0 and later, this rule replaces the Disable BlackBerry App World IT policy rule in the Security policy group.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.5
Rule introduction	• BlackBerry Enterprise Server 5.0 SP2

Disable Application Purchasing IT policy rule

Description	This rule specifies whether a BlackBerry device user can purchase applications from the BlackBerry App World storefront.
Possible values	• Yes • No
Default values	• No
Minimum requirements	• BlackBerry Device Software 4.5
Rule introduction	• BlackBerry Enterprise Server 5.0 SP2

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.

Possible values	• Yes • No
Default values	• No
Minimum requirements	• BlackBerry Device Software 4.5
Rule introduction	• BlackBerry Enterprise Server 5.0 SP2

BlackBerry Bridge policy group

Enable BlackBerry Bridge IT policy rule

Description	This rule specifies whether a BlackBerry device can run the BlackBerry Bridge app. If you set this rule to Yes, a user can run the BlackBerry Bridge app and use it to connect a companion device (for example, a BlackBerry PlayBook tablet) to the BlackBerry device. If you set this rule to No, a user cannot run the BlackBerry Bridge app and cannot use it to connect a companion device to the BlackBerry device.
Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server 5.0 SP4 • KB26294

Private Transport IT policy rule

Description	This rule specifies whether a BlackBerry device with an active BlackBerry Bridge connection can connect to the private transport (for example, your organization's BlackBerry Enterprise Server).
Related rules	The Enable BlackBerry Bridge IT policy rule affects this rule. If the Enable BlackBerry Bridge rule is set to No, this rule does not apply.
Possible values	• Allow • Disallow
Default value	• Allow
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server 5.0 SP4

Public Transport IT policy rule

Description	This rule specifies whether a BlackBerry device with an active BlackBerry Bridge connection can connect to the public transport (for example, the BlackBerry Internet Service).
Related rules	The Enable BlackBerry Bridge IT policy rule affects this rule. If the Enable BlackBerry Bridge rule is set to No, this rule does not apply.
Possible values	• Allow • Disallow
Default value	• Allow
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server 5.0 SP4

BlackBerry Messenger policy group

BBM Voice IT policy rule

Description	This rule specifies whether a BlackBerry device can use the BBM Voice feature in BlackBerry Messenger. If you set this rule to Disallow, the user cannot use the BBM Voice feature.
Possible values	• Allow • Disallow
Default value	• Allow
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server 5.0 SP4 • KB33176

Disable BlackBerry Messenger IT policy rule

Description	This rule specifies whether BlackBerry Messenger is available on a BlackBerry device.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server 4.0 SP2

Disable BlackBerry Messenger Groups IT policy rule

Description	This rule specifies whether a BlackBerry device user can participate in BlackBerry Messenger groups. Currently, you cannot audit information that members of BlackBerry Messenger groups send to each other. You can prevent users from participating in BlackBerry Messenger groups if your organization's security policies require you to audit all information that users send using BlackBerry Messenger.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.5
Rule introduction	• BlackBerry Enterprise Server 5.0 SP2 • KB19406

Disable Check for Updates IT policy rule

Description	This rule specifies whether a BlackBerry device checks automatically for a version of the BlackBerry Messenger that is more recent than the version that is currently on the device.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.5
Rule introduction	• BlackBerry Enterprise Server 5.0 SP1 • KB19406

Disable Location Requests, Responses, and Proximity Alerts IT policy rule

Description	This rule specifies whether a BlackBerry device use can use BlackBerry Messenger to make location requests, respond to location requests, or request or send proximity alerts to another user.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.5
Rule introduction	• BlackBerry Enterprise Server 5.0 SP1

Disable Server Based Contact List Synchronization IT policy rule

Description	This rule specifies whether a BlackBerry device user can store the contact list for BlackBerry Messenger in the BlackBerry Infrastructure. When the contact list is stored in the BlackBerry Infrastructure, a user who frequently switches devices can use the same synchronized contact list on all devices. If you set this rule to Yes, users cannot see the display pictures for BlackBerry Messenger contacts. Contact list synchronization is required for the display pictures for BlackBerry Messenger contacts to appear on the device.
Possible values	• Yes • No
Default value	• No

Minimum requirements	• BlackBerry Device Software 4.5
Rule introduction	• BlackBerry Enterprise Server 5.0 SP1 • KB19406

Disallow External Email Address for Server Registration IT policy rule

Description	This rule specifies whether a BlackBerry device user can register an email address with the BlackBerry Messenger server if the email address is not associated with a BlackBerry Enterprise Server.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.5
Rule introduction	• BlackBerry Enterprise Server 5.0 SP1 • KB19406

Disallow Forwarding of Contacts IT policy rule

Description	This rule specifies whether a BlackBerry device user can forward a BlackBerry Messenger contact to another user.
Possible values	• Yes • No
Default value	• No

Minimum requirements	• BlackBerry Device Software 4.6
Rule introduction	• BlackBerry Enterprise Server 4.1 SP6

Disallow Setting a Subject on Conversations IT policy rule

Description	This rule specifies whether a BlackBerry device user can type a subject for a BlackBerry Messenger conversation.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.5
Rule introduction	• BlackBerry Enterprise Server 5.0 SP1 • KB19406

Enforce Security Question in BlackBerry Messenger Invitation IT policy rule

Description	This rule specifies whether a BlackBerry device can enforce a security question for BlackBerry Messenger invitations sent as PIN messages or email messages.
Possible values	• Yes • No
Default value	• No

Minimum requirements	• BlackBerry Device Software 4.5
Rule introduction	• BlackBerry Enterprise Server 5.0 SP1 • KB19406

Messenger Audit Email Address IT policy rule

Description	This rule specifies the email address that a BlackBerry device sends BlackBerry Messenger audit reports to. Configure a value for this rule if you want to audit the use of BlackBerry Messenger in your organization's environment. Audit reports include the date and time of instant messages in UTC.
Related rules	The Messenger Audit UID IT policy rule affects this rule. The device uses the service book that you specify in the Messenger Audit UID IT policy rule to send audit reports to the email address that you specify in this rule.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server 4.0 SP2

Messenger Audit Max Report Interval IT policy rule

Description	This rule specifies the maximum amount of time (in hours) that can elapse between BlackBerry Messenger audit reports when there is no new data available. Audit reports include the date and time of instant messages in UTC.
Related rules	The Messenger Audit Email Address IT policy rule affects this rule. The BlackBerry device sends audit reports to the email address that you specify in the Messenger Audit Email Address IT policy rule.
Possible values	• 1 to 8736 hours
Default value	• 168 hours

Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server 4.0 SP2

Messenger Audit Report Interval IT policy rule

Description	This rule specifies the amount of time that can elapse between BlackBerry Messenger audit reports when there is new data available. Change this rule to a shorter interval to manage the amount of built-in media storage that BlackBerry Messenger uses. Audit reports include the date and time of instant messages in UTC.
Related rules	The Messenger Audit Email Address IT policy rule affects this rule. The BlackBerry device sends audit reports to the email address that you specify in the Messenger Audit Email Address IT policy rule.
Possible values	• 1 to 8736 hours
Default value	• 24 hours
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server 4.0 SP2

Messenger Audit UID IT policy rule

Description	This rule specifies the unique identifier of the service book that the BlackBerry device uses to send BlackBerry Messenger audit reports to the email address that you specify in the Messenger Audit Email Address IT policy rule. Audit reports include the date and time of instant messages in UTC.
Related rules	The Messenger Audit Email Address IT policy rule affects this rule. The device sends audit reports to the email address that you specify in the Messenger Audit Email Address IT policy rule.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 3.6

Rule introduction	• BlackBerry Enterprise Server 4.0 SP2

BlackBerry Pushcast policy group

The previous name of this policy group was Chalk Pushcast policy group.

Allow BlackBerry Pushcast Player Auto Update Prompt IT policy rule

Description	This rule specifies whether the BlackBerry Pushcast Player on a BlackBerry device should prompt the BlackBerry device user automatically when a new version of the BlackBerry Pushcast Player is available. The previous name of this rule was Allow Chalk Pushcast Player Auto Update Prompt IT policy rule.
Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry Enterprise Server 4.1 SP6 for Microsoft Exchange or later • BlackBerry Enterprise Server 4.1 SP5 for IBM Domino or later
Rule introduction	• BlackBerry Pushcast Console download

Allow BlackBerry Pushcast Player Roaming IT policy rule

Description	This rule specifies whether the BlackBerry Pushcast Player on a BlackBerry device can download content from the BlackBerry Pushcast Software when the device is roaming. A BlackBerry device user

	can change the value to No on the BlackBerry Pushcast Player to specify that the BlackBerry Pushcast Player cannot download content when the device is roaming even if you configure the value for this rule to Yes. If the BlackBerry Pushcast Player can connect to the BlackBerry Pushcast Software over a Wi-Fi network, the BlackBerry Pushcast Player can download content when the device is roaming even if you change the value for this rule to No. The previous name of this rule was Allow Chalk Pushcast Player Roaming IT policy rule.
Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry Enterprise Server 4.1 SP6 for Microsoft Exchange or later • BlackBerry Enterprise Server 4.1 SP5 for IBM Domino or later
Rule introduction	• BlackBerry Pushcast Console download

Allow Launch of BlackBerry Pushcast Player IT policy rule

Description	This rule specifies whether a BlackBerry device user can open the BlackBerry Pushcast Player on a BlackBerry device. The previous name of this rule was Allow Launch if Chalk Pushcast Player IT policy rule.
Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry Enterprise Server 4.1 SP6 for Microsoft Exchange or later • BlackBerry Enterprise Server 4.1 SP5 for IBM Domino or later

Rule introduction	• BlackBerry Pushcast Console download

BlackBerry Pushcast Player Default Connection Type IT policy rule

Description	This rule specifies the default connection type that the BlackBerry Pushcast Player should use to connect to the BlackBerry Pushcast Software. The previous name of this rule was Chalk Pushcast Player Default Connection Type IT policy rule.
Possible values	• BES • BIS
Default value	• BES
Minimum requirements	• BlackBerry Enterprise Server 4.1 SP6 for Microsoft Exchange or later • BlackBerry Enterprise Server 4.1 SP5 for IBM Domino or later
Rule introduction	• BlackBerry Pushcast Console download

BlackBerry Pushcast Player Default Servers List IT policy rule

Description	This rule specifies the BlackBerry Pushcast servers that the BlackBerry Pushcast Player includes in the server list on a BlackBerry device by default. If you specify a value for this rule, the BlackBerry Pushcast server that you specify is listed in the server list on the device. For example, if the URI for the BlackBerry Pushcast server is https://m.blackberry.com, specify m.blackberry.com as the value for this rule. You must separate multiple values with a comma (,).
Default value	• Null value
Rule introduction	• BlackBerry Enterprise Server 5.0 SP3

BlackBerry Pushcast Player Host URL IT policy rule

Description	This rule specifies the URL of the server (for example, https://server01.rim.com) that hosts the BlackBerry Pushcast Software. The BlackBerry Pushcast Player uses the FQDN to connect to the BlackBerry Pushcast Software. To use the BlackBerry Pushcast Player, you must configure this rule if your organization is not using m.chalknetwork.com as the server that hosts the BlackBerry Pushcast Software. The previous name of this rule was Chalk Pushcast Player Host URL IT policy rule.
Default value	• Null value
Minimum requirements	• BlackBerry Enterprise Server 4.1 SP6 for Microsoft Exchange or later • BlackBerry Enterprise Server 4.1 SP5 for IBM Domino or later
Rule introduction	• BlackBerry Pushcast Console download

BlackBerry Pushcast Player Mobile Network Data Limit IT policy rule

Description	This rule specifies the data limit that the BlackBerry Pushcast Player can use to download content from the BlackBerry Pushcast Software over the wireless network in a one-month period. If you set this rule to -1, there is no data limit. The previous name of this rule was Chalk Pushcast Player Mobile Network Data Limit IT policy rule.
Possible values	• -1 to 1,048,576 MBs
Default value	• -1
Minimum requirements	• BlackBerry Enterprise Server 4.1 SP6 for Microsoft Exchange or later • BlackBerry Enterprise Server 4.1 SP5 for IBM Domino or later

Rule introduction	• BlackBerry Pushcast Console download

Restrict BlackBerry Pushcast Player to Wi-Fi IT policy rule

Description	This rule specifies whether the BlackBerry Pushcast Player on a BlackBerry device can download content from the BlackBerry Pushcast Software when the device is not connected to a Wi-Fi network. The previous name of this rule was Restrict Chalk Pushcast Player to Wi-Fi IT policy rule.
Possible values	• Use Wi-Fi if capable • Only use Wi-Fi • No restrictions
Default value	• No restrictions
Minimum requirements	• BlackBerry Enterprise Server 4.1 SP6 for Microsoft Exchange or later • BlackBerry Enterprise Server 4.1 SP5 for IBM Domino or later
Rule introduction	• BlackBerry Pushcast Console download

BlackBerry Smart Card Reader policy group

For more information about using the BlackBerry Smart Card Reader with computers and BlackBerry devices, see the *BlackBerry Enterprise Solution Security Technical Overview* and the *BlackBerry Smart Card Reader Security Technical Overview*.

Disable Auto Reconnect To BlackBerry Smart Card Reader IT policy rule

Description	This rule specifies whether a computer or BlackBerry device previously connected to a BlackBerry Smart Card Reader can reconnect automatically.
Possible values	• Disable Auto Reconnect On BlackBerry • Disable Auto Reconnect On PC
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.0 • BlackBerry Smart Card Reader software 1.5.1
Rule introduction	• BlackBerry Enterprise Server 4.0 SP7

Force Erase All Keys on BlackBerry Disconnected Timeout IT policy rule

Description	This rule specifies whether the keys that a computer or BlackBerry device use to connect to a BlackBerry Smart Card Reader are deleted after the connection closes.
Related	The Maximum BlackBerry Disconnect Timeout IT policy rule affects this rule. The device uses this rule only if you configure the Maximum BlackBerry Disconnect Timeout IT policy rule.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.0 • BlackBerry Smart Card Reader software 1.5

Rule introduction	• BlackBerry Enterprise Server 4.0 SP5

Force Erase Key on PC Standby IT policy rule

Description	This rule specifies whether a computer deletes the key that the computer users to connect to a BlackBerry Smart Card Reader and closes the connection when the computer goes into standby mode.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.0 • BlackBerry Smart Card Reader software 1.5.1
Rule introduction	• BlackBerry Enterprise Server 4.0 SP7

Maximum BlackBerryBluetooth Traffic Inactivity Timeout IT policy rule

Description	This rule specifies the maximum time of inactivity over a Bluetooth connection that a BlackBerry Smart Card Reader and BlackBerry device permit before the BlackBerry Smart Card Reader and device delete the connection information. If you configure this rule, the BlackBerry device user can change the Inactivity Timeout to a shorter interval. If you do not configure this rule, the user can change the Inactivity Timeout field to any value. Any packet that the BlackBerry Smart Card Reader or device sends or receives over a Bluetooth connection other than the connection-heartbeat packet, resets the timeout.
Possible values	• 1 to 10,080 minutes
Default value	• Null value

Exceptions	• BlackBerry Enterprise Server for Novell GroupWise
Minimum requirements	• BlackBerry Device Software 4.0 • BlackBerry Smart Card Reader software 1.5.1
Rule introduction	• BlackBerry Enterprise Server 4.0 SP2

Maximum BlackBerry Disconnected Timeout IT policy rule

Description	This rule specifies the Disconnected Timeout. The Disconnected Timeout is the maximum time of inactivity after the Bluetooth connection between a BlackBerry device and BlackBerry Smart Card Reader closes. If you specify a value for this rule, a BlackBerry device can only change the Disconnected Timeout field on the device to a shorter interval. If you do not configure this rule, the user can change the Disconnected Timeout value to any value.
Related rules	This rule affects the Force Erase All Keys on BlackBerry Disconnected Timeout IT policy rule. The device uses the Force Erase All Keys on BlackBerry Disconnected Timeout IT policy rule only if you specify a value for this rule.
Possible values	• 0 to 604,800 seconds
Default value	• Null value
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise
Minimum requirements	• BlackBerry Device Software 4.0 • BlackBerry Smart Card Reader software 1.5
Rule introduction	• BlackBerry Enterprise Server 4.0 SP2

Maximum BlackBerry Long Term Timeout IT policy rule

Description	This rule specifies the maximum time that can elapse after a BlackBerry device and a BlackBerry Smart Card Reader connect before the device and the BlackBerry Smart Card Reader delete the connection information. If you specify a value for this rule, a BlackBerry device user can change the Long Term Timeout field to a shorter interval. If you do not specify a value for this rule, the user can change the Long Term Timeout field to any value.
Possible values	• 1 to 720 hours
Default value	• Null value
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise
Minimum requirements	• BlackBerry Device Software 4.0 • BlackBerry Smart Card Reader software 1.5.1
Rule introduction	• BlackBerry Enterprise Server 4.0 SP2

Maximum Bluetooth Encryption Key Regeneration Period IT policy rule

Description	This rule specifies the length of time that can elapse after a BlackBerry Smart Card Reader regenerates a Bluetooth encryption key if a BlackBerry device or computer is connected to the BlackBerry Smart Card Reader. If the device or computer is not connected to the BlackBerry Smart Card Reader, the BlackBerry Smart Card Reader regenerates the encryption key when the device or computer reconnects to the BlackBerry Smart Card Reader.
Possible values	• 1 to 720 hours
Default value	• Null value

Minimum requirements	• BlackBerry Device Software 4.0 • BlackBerry Smart Card Reader software 1.5.1
Rule introduction	• BlackBerry Enterprise Server 4.0 SP7

Maximum Bluetooth Range IT policy rule

Description	This rule specifies the maximum power range that a BlackBerry Smart Card Reader uses to send Bluetooth packets. The permitted range is 30% through 100%. You can configure a lower power range for a BlackBerry device or computer to communicate with a BlackBerry Smart Card Reader over a shorter distance.
Possible values	• 30% to 100%
Default value	• 100%
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise
Minimum requirements	• BlackBerry Device Software 4.0 • BlackBerry Smart Card Reader software 1.0
Rule introduction	• BlackBerry Enterprise Server 4.0 SP3

Maximum Connection Heartbeat Period IT policy rule

Description	This rule specifies the maximum amount of time for the Connection Heartbeat Period. The Maximum Connection Heartbeat Period is the amount of time that the Bluetooth connection remains open without a BlackBerry device or computer sending a heartbeat to a BlackBerry Smart Card Reader or the BlackBerry Smart Card Reader acknowledging a heartbeat. If the device or computer does not send a heartbeat or the BlackBerry Smart Card Reader does not acknowledge the heartbeat in the Connection Heartbeat Period, the Bluetooth connection closes. If you configure this rule, the BlackBerry device user can change the Connection Heartbeat Period field on a device or a computer to a shorter interval. If you do not configure this rule, the user can change the Connection Heartbeat Period field to any value.

	If you configure a short interval, Bluetooth traffic increases. The increased traffic might affect the battery-power level of the device and BlackBerry Smart Card Reader.
Related rules	The Maximum BlackBerry Disconnected Timeout IT policy rule affects this rule. You can use the Maximum BlackBerry Disconnected Timeout IT policy rule to specify the device disconnected timer. The Maximum PC Disconnected Timeout IT policy rule affects this rule. You can use the Maximum PC Disconnected Timeout IT policy rule to specify the computer disconnected timer.
Possible values	• 60 to 3600 seconds
Default value	• Null value
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise
Minimum requirements	• BlackBerry Device Software 4.0 • BlackBerry Smart Card Reader software 1.0
Rule introduction	• BlackBerry Enterprise Server 4.0 SP2

Maximum Number of BlackBerry Transactions IT policy rule

Description	This rule specifies the maximum number of transactions that can occur between a BlackBerry device and a BlackBerry Smart Card Reader before the device and BlackBerry Smart Card Reader delete the connection information. A transaction is any set of request and response packets other than a connection heartbeat packet. If you configure this rule, a BlackBerry device user can change the Number of Transactions field on the device to a lower value. If you do not configure this rule, the user can change the Number of Transactions field to any value.
Possible values	• 100 to 10,000 transactions
Default value	• Null value
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise

Minimum requirements	• BlackBerry Device Software 4.0 • BlackBerry Smart Card Reader software 1.5
Rule introduction	• BlackBerry Enterprise Server 4.0 SP2

Maximum Number of PC Pairings IT policy rule

Description	This rule specifies the maximum number of computers that can connect to a BlackBerry Smart Card Reader. If you configure this rule while computers are connected to a BlackBerry Smart Card Reader and more than the maximum number of computers are connected, the BlackBerry Smart Card Reader closes connections with the last computers to connect.
Possible values	• 0 to 65,535 computers
Default value	• Null value
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise
Minimum requirements	• BlackBerry Smart Card Reader software 1.5
Rule introduction	• BlackBerry Enterprise Server 4.0 SP5

Maximum Number of PC Transactions IT policy rule

Description	This rule specifies the maximum number of transactions that can occur between a computer and a BlackBerry Smart Card Reader before the computer and BlackBerry Smart Card Reader delete the connection information. A transaction is any set of request and response packets other than a connection heartbeat packet. If you configure this rule, a BlackBerry device user can change the Number of Transactions field in the BlackBerry Smart Card Reader options on a computer to a lower value. If you do not configure this rule, the user can change the Number of Transactions field to any value.
Possible values	• 100 to 10,000 transactions

Default value	• Null value
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise
Minimum requirements	• BlackBerry Smart Card Reader software 1.5
Rule introduction	• BlackBerry Enterprise Server 4.0 SP5

Maximum PC Bluetooth Traffic Inactivity Timeout IT policy rule

Description	This rule specifies the maximum time of inactivity over a Bluetooth connection that a BlackBerry Smart Card Reader and computer permit before the BlackBerry Smart Card Reader and computer delete the connection information. If you configure this rule, the BlackBerry device user can change the Inactivity Timeout field in the BlackBerry Smart Card Reader options on the computer to a shorter interval. If you do not configure this rule, the user can change the Inactivity Timeout field to any value. Any packet that the BlackBerry Smart Card Reader or computer sends or receives over a Bluetooth connection other than the connection-heartbeat packet, resets the timeout.
Possible values	• 1 to 10,080 minutes
Default value	• Null value
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise
Minimum requirements	• BlackBerry Smart Card Reader software 1.5
Rule introduction	• BlackBerry Enterprise Server 4.0 SP5

Maximum PC Disconnected Timeout IT policy rule

Description	This rule specifies the maximum time that can elapse after a BlackBerry Smart Card Reader and computer close a Bluetooth connection before the BlackBerry Smart Card Reader and computer delete the connection information. If you configure this rule, the BlackBerry device user can change the Disconnected Timeout field in the BlackBerry Smart Card Reader options on a computer to a shorter interval. If you do not configure this rule, the user can change the Disconnected Timeout field to any value.
Possible values	• 0 to 604,800 seconds
Default value	• Null value
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise
Minimum requirements	• BlackBerry Smart Card Reader software 1.5
Rule introduction	• BlackBerry Enterprise Server 4.0 SP5

Maximum PC Long Term Timeout IT policy rule

Description	This rule specifies the maximum time that can elapse after a BlackBerry Smart Card Reader and computer connect before the BlackBerry Smart Card Reader and computer delete the connection information. If you configure this rule, a BlackBerry device user can change the Long Term Timeout field in the BlackBerry Smart Card Reader options on a computer to a shorter interval. If you do not configure this rule, the user can change the Long Term Timeout field to any value.
Related IT policy rules	This rule is related to the Maximum PC Bluetooth Traffic Inactivity Timeout IT policy rule.
Possible values	• 1 to 720 hours
Default value	• Null value

Exceptions	• BlackBerry Enterprise Server for Novell GroupWise
Minimum requirements	• BlackBerry Smart Card Reader software 1.5
Rule introduction	• BlackBerry Enterprise Server 4.0 SP5

Maximum Smart Card Not Present Timeout IT policy rule

Description	This rule specifies the maximum time that can elapse after a BlackBerry device user removes a smart card from a BlackBerry Smart Card Reader before the BlackBerry device and BlackBerry Smart Card Readerdelete the connection information. If you configure this rule, the user can change the Card Not Present Timeout field on the device to a lower value. If you do not configure this rule, the user can change the Card Not Present Timeout value on the device to any value.
Possible values	• 0 to 86,400 seconds
Default value	• Null value
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise
Minimum requirements	• BlackBerry Device Software 4.0 • BlackBerry Smart Card Reader software 1.5
Rule introduction	• BlackBerry Enterprise Server 4.0 SP2

Minimum PIN Entry Mode IT policy rule

Description	This rule specifies the minimum PIN entry mode that is required when a BlackBerry device user connects a BlackBerry Smart Card Reader and a BlackBerry device or computer. The BlackBerry Enterprise Server enforces the minimum PIN entry mode when the user types the user-authenticator password (smart card PIN) during the Bluetooth connection process.

Possible values	• Alphanumeric lowercase • Alphanumeric mixed case • Numeric
Default value	• Numeric
Minimum requirements	• BlackBerry Device Software 5.0 • BlackBerry Smart Card Reader 2.0
Rule introduction	• BlackBerry Enterprise Server 5.0 • KB19406

BlackBerry Unite! policy group

Disable Download Manager IT policy rule

Description	This rule specifies whether to prevent the Download Manager for the BlackBerry Unite! software from running on a BlackBerry device.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.2.2
Rule introduction	• BlackBerry Enterprise Server 4.1 SP6

Disable Unite! Applications IT policy rule

Description	This rule specifies whether to prevent applications for the BlackBerry Unite! software from running on a BlackBerry device.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.2.2
Rule introduction	• BlackBerry Enterprise Server 4.1 SP6

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*.

Allow Outgoing Calls IT policy rule

Description	This rule specifies whether a BlackBerry device user can place outgoing calls from a BlackBerry device using Bluetooth technology.
Possible values	• Always • Never • Only
Default value	• Always

Minimum requirements	• BlackBerry Device Software 4.0.2
Rule introduction	• BlackBerry Enterprise Server 4.0 SP1

Disable Address Book Transfer IT policy rule

Description	This rule specifies whether to prevent a BlackBerry device from exchanging address-book data with a supported Bluetooth device.
Possible values	• Yes • No
Default values	• Yes in the Advanced security IT policy and Advanced Security with No 3rd Party Applications IT policy • No in all other preconfigured IT policies
Minimum requirements	• BlackBerry Device Software 4.1
Rule introduction	• BlackBerry Enterprise Server 4.0 SP3

Disable Advanced Audio Distribution Profile IT policy rule

Description	This rule specifies whether a BlackBerry device can use the Bluetooth A2DP.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.2.2

Rule introduction	• BlackBerry Enterprise Server 4.1 SP4

Disable Audio/Video Remote Control Profile IT policy rule

Description	This rule specifies whether a BlackBerry device can use the Bluetooth AVRCP.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.2.2
Rule introduction	• BlackBerry Enterprise Server 4.1 SP4

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
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise only with devices that are running BlackBerry Device Software 4.0 and later
Minimum requirements	• BlackBerry Device Software 3.8

Rule introduction	• BlackBerry Enterprise Server 4.0

Disable Desktop Connectivity IT policy rule

Description	This rule specifies whether to prevent a BlackBerry device from using Bluetooth technology to connect to the BlackBerry Desktop Software.
Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry Device Software 4.1
Rule introduction	• BlackBerry Enterprise Server 4.0 SP3

Disable Dial-Up Networking IT policy rule

Description	This rule specifies whether to prevent a BlackBerry device from using the Bluetooth DUN profile.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.2
Rule introduction	• BlackBerry Enterprise Server 4.0 SP6

Disable Discoverable Mode IT policy rule

Description	This rule specifies whether to prevent a BlackBerry device user from making a BlackBerry device discoverable. A BlackBerry device that is discoverable can be found by other Bluetooth devices within range of the device.
Possible values	• Yes • No
Default values	• No in the Default IT policy and Basic password security IT policy • Yes in all other preconfigured IT policies
Minimum requirements	• BlackBerry Device Software 4.0.2
Rule introduction	• BlackBerry Enterprise Server 4.0 SP1

Disable File Transfer IT policy rule

Description	This rule specifies whether to prevent a BlackBerry device from exchanging files with supported Bluetooth OBEX devices.
Possible values	• Yes • No
Default values	• Yes in the Advanced security IT policy and Advanced security with no 3rd party applications IT policy • No in all other preconfigured IT policies
Minimum requirements	• BlackBerry Device Software 4.2
Rule introduction	• BlackBerry Enterprise Server 4.0 SP6

Disable Handsfree Profile IT policy rule

Description	This rule specifies whether a BlackBerry device can use the Bluetooth HFP. The device can use the Bluetooth HFP to connect to most car kits and some headsets.
Possible values	• Yes • No
Default value	• No
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise only in BlackBerry Device Software 4.0 and later
Minimum requirements	• BlackBerry Device Software 3.8
Rule introduction	• BlackBerry Enterprise Server 4.0

Disable Headset Profile IT policy rule

Description	This rule specifies whether a BlackBerry device can use the Bluetooth HSP. The device can use the Bluetooth HSP to connect to most headsets and some car kits.
Possible values	• Yes • No
Default value	• No
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise only with devices running BlackBerry Device Software 4.0 and later
Minimum requirements	• BlackBerry Device Software 3.8

Rule introduction	• BlackBerry Enterprise Server 4.0

Disable Message Access Profile IT policy rule

Description	This rule specifies whether a Bluetooth device that uses MAP can retrieve email messages and SMS text messages from, or upload email messages and SMS text messages to, a BlackBerry device. You can use this rule to prevent the BlackBerry device from running MAP services and to prevent a Bluetooth device that uses MAP from communicating with a BlackBerry device.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server 5.0 SP2

Disable Pairing IT policy rule

Description	This rule specifies whether a BlackBerry device can connect to a Bluetooth device. After a BlackBerry device connects to a Bluetooth device, you can use this rule to prevent the BlackBerry device from connecting to other Bluetooth devices.
Possible values	• Yes • No
Default value	• No
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise only with devices running BlackBerry Device Software 4.0 and later
Minimum requirements	• BlackBerry Device Software 3.8

Rule introduction	• BlackBerry Enterprise Server 4.0

Disable Serial Port Profile IT policy rule

Description	This rule specifies whether a BlackBerry device can use the Bluetooth SPP. A BlackBerry device uses the Bluetooth SPP to establish a serial connection with a Bluetooth device that uses a serial port interface.
Possible values	• Yes • No
Default values	• Yes in the Advanced security IT policy and Advanced security with no 3rd party applications IT policy. • No in all other preconfigured IT policies
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise only with devices running BlackBerry Device Software 4.0 and later
Minimum requirements	• BlackBerry Device Software 3.8
Rule introduction	• BlackBerry Enterprise Server 4.0

Disable SIM Access Profile IT policy rule

Description	This rule specifies whether to prevent a BlackBerry device from using the Bluetooth SIM Access Profile. A car kit might require the Bluetooth SIM Access Profile to dial a number.
Possible values	• Yes • No
Default value	• No

Minimum requirements	• BlackBerry Device Software 4.6
Rule introduction	• BlackBerry Enterprise Server 4.1 SP6

Disable Wireless Bypass IT policy rule

Description	This rule specifies whether to prevent wireless bypass using Bluetooth technology on a BlackBerry device.
Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry Device Software 4.1
Rule introduction	• BlackBerry Enterprise Server 4.0 SP3

Force CHAP Authentication on Bluetooth Link IT policy rule

Description	This rule specifies whether a BlackBerry device must use CHAP authentication to connect to a computer using a Bluetooth serial connection.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Desktop Software 4.2.2 • BlackBerry Device Software 4.2.2

Rule introduction	• BlackBerry Enterprise Server 4.1 SP4

Human Interface Device Profile IT policy rule

Description	This rule specifies whether a Bluetooth enabled BlackBerry device can use the Human Interface Device Profile (HID) to act as a Bluetooth keyboard or mouse.
Possible values	• Allow • Disallow
Default value	• Allow
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server 5.0 SP4

Limit Discoverable Time IT policy rule

Description	This rule specifies whether a BlackBerry device user must select a time limit for the Bluetooth discoverable mode on a BlackBerry device.
Related rules	The Disable Discoverable Mode IT policy rule affects this rule. A device uses this rule only if you configure the Disable Discovery Mode IT policy rule to No.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.5
Rule introduction	• BlackBerry Enterprise Server 4.1 SP5

Minimum Encryption Key Length IT policy rule

Description	This rule specifies the minimum encryption-key length that a BlackBerry device uses to encrypt Bluetooth connections.
Possible values	• 1 to 16 bytes
Default value	• 1 byte
Minimum requirements	• BlackBerry Device Software 4.5
Rule introduction	• BlackBerry Enterprise Server 4.1 SP5

Require Encryption IT policy rule

Description	This rule specifies whether a BlackBerry device uses Bluetooth encryption for all connections.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.1
Rule introduction	• BlackBerry Enterprise Server 4.0 SP4

Require LED Connection Indicator IT policy rule

Description	This rule specifies whether the LED must flash when a BlackBerry device is connected to a Bluetooth device.

Possible values	• Yes • No
Default values	• Yes in the Advanced security IT policy and Advanced security with no 3rd party applications IT policy • No in all other preconfigured IT policies
Minimum requirements	• BlackBerry Device Software 4.2
Rule introduction	• BlackBerry Enterprise Server 4.0 SP6

Require Password for Discoverable Mode IT policy rule

Description	This rule specifies whether a BlackBerry device user must type the BlackBerry device password before the BlackBerry device can be discovered by Bluetooth devices.
Related rules	The Password Required IT policy rule affects this rule. A BlackBerry device uses this rule only if the Password Required IT policy rule is configured to Yes.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.1
Rule introduction	• BlackBerry Enterprise Server 4.0 SP3

Require Password for Enabling Bluetooth Support IT policy rule

Description	This rule specifies whether a BlackBerry device user must type the BlackBerry device password to turn on Bluetooth technology.
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 value	• No
Minimum requirements	• BlackBerry Device Software 4.1
Rule introduction	• BlackBerry Enterprise Server 4.0 SP3

Browser policy group

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

Allow Application Download Services IT policy rule

Description	This rule specifies whether the icon for an application download service appear on a BlackBerry device when the wireless service provider assigns a service to the device and the appropriate service books are present on the device.
Possible values	• Yes • No

Default value	• Yes
Minimum requirements	• BlackBerry Device Software 4.3
Rule introduction	• BlackBerry Enterprise Server 4.1 SP5

Allow Hotspot Browser IT policy rule

Description	This rule specifies whether a BlackBerry device can access the hotspot browser.
Possible values	• Allow • Disallow • Only for Hotspot Login
Default value	• Allow
Minimum requirements	• BlackBerry Device Software 4.6
Rule introduction	• BlackBerry Enterprise Server 4.1 SP6

Allow IBS Browser IT policy rule

Description	This rule specifies whether an icon for BlackBerry Internet Service Browsing appears on a BlackBerry device if the appropriate service books are present for BlackBerry Internet Service Browsing.
Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry Device Software 4.0

Rule introduction	• BlackBerry Enterprise Server 4.0 SP1

Disable Auto Synchronization in Browser IT policy rule

Description	This rule specifies whether to prevent a BlackBerry device user from configuring intervals for automatic synchronization of the bookmark list in the BlackBerry Browser.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.2
Rule introduction	• BlackBerry Enterprise Server 4.0 SP6

Disable JavaScript in Browser IT policy rule

Description	This rule specifies whether to permit the execution of JavaScript code on a BlackBerry device.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0

Disable Pre-IETF WebSocket Connections in Browser IT policy rule

Description	This rule specifies whether the browser on a BlackBerry device prevents the creation of connections that use a pre-IETF version of the WebSocket protocol.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry 7
Rule introduction	• BlackBerry Enterprise Server 5.0 SP4 • KB28284

Download Images URL IT policy rule

Description	This rule specifies a web address that the BlackBerry device visits automatically when a BlackBerry device user clicks Download Images on the device.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.1
Rule introduction	• BlackBerry Enterprise Server 4.0 SP3

Download Themes URL IT policy rule

Description	This rule specifies a web address that the BlackBerry device visits automatically when a BlackBerry device user clicks Download Themes on the device.

Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.1
Rule introduction	• BlackBerry Enterprise Server 4.0 SP3

Download Tunes URL IT policy rule

Description	This rule specifies a web address that the BlackBerry device visits automatically when a BlackBerry device user clicks Download Ring Tunes on the device.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.1
Rule introduction	• BlackBerry Enterprise Server 4.0 SP3

IETF WebSocket Connections in Browser IT policy rule

Description	This rule specifies whether the browser on a BlackBerry device allows IETF WebSocket connections.
Possible values	• Allow • Disallow
Default value	• Allow
Minimum requirements	• BlackBerry 7.1
Rule introduction	• BlackBerry Enterprise Server 5.0 SP4 • KB29510

MDS Browser BSM Enabled IT policy rule

Description	This rule specifies whether the browser session manager is turned on in the BlackBerry Browser. The browser session manager is designed to improve BlackBerry Browser performance by helping the BlackBerry MDS Connection Service use the BlackBerry Browser cache.
Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry Device Software 4.0.2
Rule introduction	• BlackBerry Enterprise Server 4.0 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 4.0 SP6

MDS Browser HTML Tables Enabled IT policy rule

Description	This rule specifies whether support for HTML tables in the BlackBerry Browser is turned on. This rule became obsolete in BlackBerry Device Software 4.6.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.0.2
Rule introduction	• BlackBerry Enterprise Server 4.0 SP2

MDS Browser Style Sheets Enabled IT policy rule

Description	This rule specifies whether style sheets in the BlackBerry Browser are turned on. This rule became obsolete in BlackBerry Device Software 4.6.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.0.2
Rule introduction	• BlackBerry Enterprise Server 4.0 SP2

MDS Browser Title IT policy rule

Description	This rule specifies the name for the BlackBerry Browser icon that appears on the Home screen.
Default value	• BlackBerry Browser
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server for Microsoft Exchange 3.6 • BlackBerry Enterprise Server for IBM Domino 4.0 • BlackBerry Enterprise Server for Novell GroupWise 4.0

MDS Browser JavaScript Enabled IT policy rule

Description	This rule specifies whether JavaScript in the BlackBerry Browser is turned on. This rule became obsolete in BlackBerry Device Software 6.0.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.0.2
Rule introduction	• BlackBerry Enterprise Server 4.0 SP2

MDS Browser Use Separate Icon IT policy rule

Description	This rule specifies whether an icon for the BlackBerry Browser appears on the Home screen of the BlackBerry device.

Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.2
Rule introduction	• BlackBerry Enterprise Server 4.0 SP6

SecureKey Browser Plug-in IT policy rule

Description	This rule specifies whether a BlackBerry device supports the SecureKey browser plug-in and allows access to HTTPS traffic through the SecureKey Browser API.
Possible values	• Allow • Disallow
Default value	• Allow
Minimum requirements	• BlackBerry 7.1
Rule introduction	• BlackBerry Enterprise Server 5.0 SP4 • KB29510

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 4.0 SP6

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 4.1 SP5

Certificate Synchronization policy group

The rules in the Certificate Synchronization policy group apply to the certificate search and retrieval features of the S/MIME Support Package for BlackBerry smartphones.

Random Source URL IT policy rule

Description	This rule specifies a web address that produces random data (for example, a website for a white-noise machine). If the S/MIME Support Package for BlackBerry smartphones 4.0 or later is installed on a BlackBerry device, the certificate synchronization tool that is part of the BlackBerry Desktop Manager can use the web address to retrieve random data to add to a device.
Default value	• Null value
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise
Minimum requirements	• S/MIME Support Package for BlackBerry smartphones 4.0 • BlackBerry Desktop Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0

User Can Disable Automatic RNG Initialization IT policy rule

Description	This rule specifies whether a BlackBerry device user can stop the BlackBerry Desktop Software from starting the random-number generator on a BlackBerry device automatically.
Possible values	• Yes • No
Default setting	• Yes
Minimum requirements	• BlackBerry Desktop Software 4.3
Rule introduction	• BlackBerry Enterprise Server 4.1 SP5

Certification Authority Profile policy group

The rules in the Certification Authority Profile policy group are used to create a certification authority profile for wireless certificate requests.

The previous name of this policy group was Certificate Authority Profile policy group.

Allow Private Key Export IT policy rule

Description	This rule specifies whether to prevent a BlackBerry device user from exporting private keys that are included in the certification authority profile. A user can export private keys using the BlackBerry Desktop Manager to back up BlackBerry device data or to synchronize certificates.
Related rules	The Disable Key Store Backup IT policy rule affects this rule. A device uses this rule only if the Disable Key Store Backup IT policy rule is configured to No.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server 5.0

Certificate Enrollment Delay IT policy rule

Description	This rule specifies the time that must elapse before a BlackBerry device can initiate the certificate enrollment process. The device selects a time randomly within this specified time period to start the certificate enrollment process so that the BlackBerry Enterprise Server receives certificate enrollment requests at different times. If the initial certificate enrollment process does not complete, the device uses this rule to specify a time to retry the certificate enrollment process.

Possible values	• 0 to 24 hours
Default value	• 1 hour
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server 5.0

Certificate Expiry Window IT policy rule

Description	This rule specifies the number of days before a certificate expires that a BlackBerry device generates a new certificate enrollment request to replace the expiring certificate.
Possible values	• 1 to 30 days
Default value	• 7 days
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server 5.0

Certification Authority Host IT policy rule

Description	This rule specifies the name of the certification authority server that is required in the certification authority profile (for example, http://<*server*>.<*domain*>). The previous name of this rule was Certificate Authority Host IT policy rule.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 5.0

Rule introduction	• BlackBerry Enterprise Server 5.0

Certification Authority Port IT policy rule

Description	This rule specifies the port number that the BlackBerry MDS Connection Service can use to connect to the certification authority. The previous name of this rule was Certificate Authority Port IT policy rule.
Possible values	• 0 to 65,535
Default value	• 80
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server 5.0

Certification Authority Profile Name IT policy rule

Description	This rule specifies a name for the certification authority profile that a BlackBerry device requires for certificate enrollment requests over a wireless network. If you change this rule after the BlackBerry Enterprise Server sends the certification authority profile to the device and you resend the IT policy, the device restarts the certificate enrollment process. The previous name of this rule was Certificate Authority Profile Name IT policy rule.
Possible values	• 0 to 32 characters
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server 5.0

Certification Authority Profile Automatic Enrollment IT policy rule

Description	This rule specifies whether the certificate authority profile starts the enrollment process automatically for a BlackBerry device. The previous name of this rule was Certificate Authority Profile Required IT policy rule.
Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server 5.0

Certification Authority Type IT policy rule

Description	This rule specifies the type of certification authority that the BlackBerry MDS Connection Service can access in your organization's environment. The previous name of this rule was Certificate Authority Type IT policy rule.
Possible values	• Microsoft Enterprise certification authority • Microsoft stand-alone certification authority • RSA certification authority
Default value	• Microsoft Enterprise certification authority
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server 5.0

Common Name Components IT policy rule

Description	This rule specifies the information that appears in the common name of the certificate that the certification authority issues to a BlackBerry device user.
Related rules	The Certification Authority Type IT policy rule affects this rule. If you change the Certification Authority Type IT policy rule to Microsoft Enterprise certification authority and the Microsoft certification authority uses a template to build the subject name for the certificate from the Microsoft Active Directory, a BlackBerry device does not use this rule.
Possible values	• User Name • Device PIN • Local Email Address
Default value	• User Name • Device PIN
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server 5.0

Custom Microsoft Certification Authority Certificate Template IT policy rule

Description	This rule specifies a custom certificate template for the Microsoft Enterprise certification authority. The previous name of this rule was Custom Microsoft Certificate Authority Certificate Template IT policy rule.
Related rules	This rule affects the Microsoft Certification Authority Certificate Template IT policy rule. If you configure this rule, a BlackBerry device does not use the Microsoft Certification Authority Certificate Template IT policy rule. The Certification Authority Type IT policy rule affects this rule. A device uses this rule only if the Certification Authority Type IT policy rule is configured to Microsoft Enterprise.

Default value	• Null value
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server 5.0

Distinguished Name Components IT policy rule

Description	This rule specifies, in a comma-delimited list, the components that must appear in the distinguished name of the certificate (for example, C=Country, O=Organization, OU=Organizational Unit).
Related rules	The Certification Authority Type IT policy rule affects this rule. If you change the Certification Authority Type IT policy rule to Microsoft Enterprise, and the Microsoft certification authority uses a template to build the subject name of the certificate from the Microsoft Active Directory, a BlackBerry device does not use this rule.
Possible values	• C=<*Country*> • L=<*Locality*> • O=<*Organization*> • OU=<*Organizational_unit*> • ST=<*State_or_Province*>
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server 5.0

Key Algorithm IT policy rule

Description	This rule specifies the algorithm that a BlackBerry device uses to generate a public-private key pair.

Possible values	• RSA • DSA
Default value	• RSA
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server 5.0

Key Length IT policy rule

Description	This rule specifies the size of the key that a BlackBerry device generates. If you configure an unsupported key size, the device chooses the next strongest key size and generates the key.
Related rules	The Key Algorithm IT policy rule affects this rule. If you change the Key Algorithm rule to RSA, you must configure the key size to be a multiple of 64. If you change the Key Algorithm rule to DSA, you must configure the key size to be 512,768, or 1024 bits.
Possible values	• 512 to 16,384 bits
Default value	• 1024 bits
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server 5.0

Microsoft Certification Authority Certificate Template IT policy rule

Description	This rule specifies the certificate template that the Microsoft Enterprise certification authority uses to create a certificate. The previous name of this rule was Microsoft Certificate Authority Certificate Template IT policy rule.

Related rules	The Certification Authority Type IT policy rule affects this rule. If you configure the Certification Authority Type IT policy rule to Microsoft Stand-alone or RSA, a BlackBerry device does not use this rule.
Possible values	• Authenticated session • Smart Card user • User certificate
Default value	• User certificate
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server 5.0

RSA Certification Authority Certificate ID IT policy rule

Description	This rule specifies the MD5 certificate ID that is assigned to the RSA certification authority. The previous name of this rule was RSA Certificate Authority Certificate ID IT policy rule.
Related rules	The Certification Authority Type IT policy rule affects this rule. A BlackBerry device uses this rule only if you change the Certification Authority Type IT policy rule to RSA.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server 5.0

RSA Jurisdiction ID IT policy rule

Description	This rule specifies the unique domain ID that you assign to the RSA certification authority.
Related rules	The Certification Authority Type IT policy rule affects this rule. A BlackBerry device uses this rule only if you configure the Certification Authority Type IT policy rule to RSA.

Default value	• Null value
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server 5.0

Common policy group

Confirm On Send IT policy rule

Description	This rule specifies the text that a BlackBerry device user must confirm on a BlackBerry device before the user sends an email message, PIN message, SMS text message, or MMS message. If you do not specify text for this rule, the device does not prompt the user for confirmation.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0

Disable FM Radio IT policy rule

Description	This rule specifies whether a BlackBerry device user can use the FM radio on a BlackBerry device. If this rule is set to Yes, a user cannot listen to FM radio stations on a device.
Possible values	• Yes • No
Default value	• No

Minimum requirements	• BlackBerry 7.1
Rule introduction	• BlackBerry Enterprise Server 5.0 SP4 • KB29510

Disable Kodiak PTT IT policy rule

Description	This rule specifies whether a BlackBerry device user can use Kodiak PTT on a supported BlackBerry device.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.2
Rule introduction	• BlackBerry Enterprise Server 4.0 SP6

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*.
Related rules	The Firewall Block Incoming Messages IT policy rule affects this rule. To block incoming MMS messages, in the Security policy group, configure the Firewall Block Incoming Messages IT policy rule.
Possible values	• Yes • No
Default value	• No

Minimum requirements	• BlackBerry Device Software 4.0.2
Rule introduction	• BlackBerry Enterprise Server 4.0

Disable Voice-Activated Dialing IT policy rule

Description	This rule specifies whether voice dialing is available on a BlackBerry device.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.2
Rule introduction	• BlackBerry Enterprise Server 4.0 SP6

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 4.1 SP5

Enable Simultaneous Phone and Data IT policy rule

Description	This rule specifies whether a BlackBerry device user can send and receive data during a call.
Possible values	• 0 to 2
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.6
Rule introduction	• BlackBerry Enterprise Server 4.1 SP6

IT Policy Notification IT policy rule

Description	This rule specifies whether warnings about changes to an IT policy appear to a BlackBerry device user.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0

Lock Owner Info IT policy rule

Description	This rule specifies whether a BlackBerry device user can change the owner information on a BlackBerry device. You can lock the Information field, the Name field, or both fields. You can overwrite the owner information by sending the Set Owner Information IT administration command to the device.

Related rules	This rule affects the Set Owner Info IT policy rule. If you set this rule to Lock Information text or Lock both Name and Information text, you must specify the owner information in the Set Owner Info IT policy rule. This rule affects the Set Owner Name IT policy rule. If you set this rule to Lock Name text or Lock both Name and Information text, you must specify the owner information in the Set Owner Name IT policy rule.
Possible values	• Lock Information text • Lock Name text • Lock both Name and Information text
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0

Set Owner Info IT policy rule

Description	This rule specifies the owner information that appears on a BlackBerry device. You can overwrite the owner information by sending the Set Owner Information IT administration command to the device.
Related rules	The Lock Owner Info IT policy rule affects this rule. You must set the Lock Owner Info IT policy rule to Lock Information text or Lock both Name and Information text for this rule to apply to the device.
Possible values	• 0 to 127 characters
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0

Set Owner Name IT policy rule

Description	This rule specifies the owner name that appears on a BlackBerry device. You can overwrite the owner information by sending the Set Owner Information IT administration command to a device.
Related rules	The Lock Owner Info IT policy rule affects this rule. You must set the Lock Owner Info IT policy rule to Lock Name text or Lock both Name and Information text for this rule to apply to the device.
Possible values	• 0 to 39 characters
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0

Companion Devices policy group

BlackBerry PlayBook Log Submission IT policy rule

Description	This rule specifies whether a BlackBerry PlayBook tablet that is connected to a BlackBerry smartphone using the BlackBerry Bridge App can generate and send log files to the BlackBerry Technical Solution Center using the BlackBerry Bridge connection.
Related rules	The Enable BlackBerry Bridge IT policy rule affects this rule. If the Enable BlackBerry Bridge rule is set to No, this rule does not apply.
Possible values	• Enable • Disable
Default value	• Enable

Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server 5.0 SP4 • KB26294

Date and Time IT policy group

Automatic Time Zone Change Detection IT policy rule

Description	This rule specifies whether a BlackBerry device can update the time-zone setting automatically using the information that it receives from the wireless network. For example, if a BlackBerry device user travels to a different time zone, by default, the device prompts the user to update the time zone.
Possible values	• On • Off • Prompt
Default value	• Prompt
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server 5.0 SP1

Enable Time Zone Definitions Update IT policy rule

Description	This rule specifies whether a BlackBerry device can update time-zone definitions over the wireless network when a BlackBerry device user requests a update to the time-zone definitions.
Possible values	• Yes • No

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

Periodic Time Synchronization IT policy rule

Description	This rule specifies whether a BlackBerry device can automatically synchronize its clock with the wireless network.
Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server 4.1 SP7

Time Zone Definitions Automatic Update Interval IT policy rule

Description	This rule specifies the length of time between automatic updates of time-zone definitions on a BlackBerry device. Specify a value for this rule to turn on automatic updates of time-zone definitions.
Possible values	• 0 to 365 days
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 5.0

Rule introduction	• BlackBerry Enterprise Server 5.0 SP1

Time Zone Definitions Update Server IT policy rule

Description	This rule specifies the FQDN of the web server that a BlackBerry device can retrieve updates to time-zone definitions from.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server 5.0 SP1

Desktop policy group

Allow BlackBerry Desktop Software Statistics IT policy rule

Description	This rule specifies whether the BlackBerry Desktop Software can send usage statistics to Research In Motion when a BlackBerry device is connected to a computer.
Possible values	• Yes • No
Default value	• Yes
Exceptions	• BlackBerry Desktop Software 6.0 • BlackBerry Enterprise Server for Novell GroupWise

Minimum requirements	• BlackBerry Desktop Manager 5.0
Rule introduction	• BlackBerry Enterprise Server 4.1 SP7

Allow External Device Software Servers IT policy rule

Description	This rule specifies whether the BlackBerry Device Software can receive updates from servers that are hosted outside your organization.
Possible values	• Yes • No
Default value	• No
Exceptions	• BlackBerry Desktop Software 6.0 • BlackBerry Enterprise Server for Novell GroupWise
Minimum requirements	• BlackBerry Desktop Manager 4.7
Rule introduction	• BlackBerry Enterprise Server 4.1 SP7

Allow IP Modem application IT policy rule

Description	This rule specifies whether a BlackBerry device user can use the IP modem application in the BlackBerry Desktop Software. If you change this rule to No, the BlackBerry Desktop Software does not display the IP modem application.
Possible values	• Yes • No
Default value	• Yes

Exceptions	• BlackBerry Desktop Software 6.0 • BlackBerry Enterprise Server for Novell GroupWise
Minimum requirements	• BlackBerry Desktop Manager 5.0.1
Rule introduction	• BlackBerry Enterprise Server 5.0 SP2

Allow Personal Folder Reconciliation IT policy rule

Description	This rule specifies whether a BlackBerry device can synchronize email messages that are in personal folders over a serial connection or USB connection.
Possible values	• Yes • No
Default value	• Yes
Exceptions	• BlackBerry Desktop Software 6.0 and 6.0.1 • BlackBerry Enterprise Server for Novell GroupWise
Minimum requirements	• BlackBerry Desktop Manager 4.7
Rule introduction	• BlackBerry Enterprise Server 4.1 SP7

Desktop Allow Desktop Add-ins IT policy rule

Description	This rule specifies whether the BlackBerry Desktop Software can run add-on applications, such as third-party COM-based extensions that access BlackBerry device databases during synchronization.
Possible values	• Yes • No

Default value	• Yes
Exceptions	• BlackBerry Desktop Software 6.0 • BlackBerry Enterprise Server for Novell GroupWise
Minimum requirements	• BlackBerry Desktop Manager 3.6
Rule introduction	• BlackBerry Enterprise Server 3.5 for Microsoft Exchange • BlackBerry Enterprise Server 4.0 for IBM Domino

Desktop Allow Device Switch IT policy rule

Description	This rule specifies whether BlackBerry Desktop Software users or BlackBerry Web Desktop Manager users can switch BlackBerry devices.
Related rules	The Enterprise Service Policy overrides this rule. For more information about using the Enterprise Service Policy, see the *BlackBerry Enterprise Solution Security Technical Overview*.
Possible values	• Yes • No
Default value	• Yes
Exceptions	• BlackBerry Desktop Software 6.0 • BlackBerry Enterprise Server for Novell GroupWise only with BlackBerry Web Desktop Manager
Minimum requirements	• BlackBerry Desktop Manager 3.5 or BlackBerry Web Desktop Manager 1.0
Rule introduction	• BlackBerry Enterprise Server 3.5 for Microsoft Exchange • BlackBerry Enterprise Server 4.0 for IBM Domino • BlackBerry Enterprise Server 4.0 for Novell GroupWise

Desktop Password Cache Timeout IT policy rule

Description	This rule specifies the length of time that the BlackBerry Desktop Software or BlackBerry Web Desktop Manager caches a BlackBerry device password in memory. If you change this rule to 0, the device clears the password from memory when a BlackBerry device user disconnects the device from a computer, regardless of the length of time that the device was connected to the computer.
Related rules	The Password Required IT policy rule affects this rule. The device uses this rule only if you configure the Password Required IT policy rule to Yes.
Possible values	• 0 to 720 minutes
Default value	• 10 minutes
Exceptions	• BlackBerry Desktop Software 6.0 • BlackBerry Enterprise Server for Novell GroupWise only with BlackBerry Web Desktop Manager
Minimum requirements	• BlackBerry Desktop Manager 3.5 or BlackBerry Web Desktop Manager 1.0
Rule introduction	• BlackBerry Enterprise Server 3.5 for Microsoft Exchange • BlackBerry Enterprise Server 4.0 for IBM Domino • BlackBerry Enterprise Server 4.0 for Novell GroupWise

Disable Check For Updates Link IT policy rule

Description	This rule specifies whether the Check for updates link in the BlackBerry Desktop Software is available.
Possible values	• Yes • No
Default value	• No
Exceptions	• BlackBerry Desktop Software 6.0

Minimum requirements	• BlackBerry Desktop Manager 4.5
Rule introduction	• BlackBerry Enterprise Server 4.1 SP5

Disable Media Manager IT policy rule

Description	This rule specifies whether the media manager tool in the BlackBerry Desktop Software is available.
Possible values	• Yes • No
Default value	• No
Exceptions	• BlackBerry Desktop Software 6.0 • BlackBerry Enterprise Server for Novell GroupWise
Minimum requirements	• BlackBerry Desktop Manager 4.2
Rule introduction	• BlackBerry Enterprise Server 4.0 SP6

Disable Media Synchronization IT policy rule

Description	This rule specifies whether BlackBerry Media Sync is available in the BlackBerry Desktop Software.
Possible values	• Yes • No
Default value	• No
Exceptions	• BlackBerry Desktop Software 6.0 • BlackBerry Enterprise Server for Novell GroupWise

Minimum requirements	• BlackBerry Desktop Manager 4.6
Rule introduction	• BlackBerry Enterprise Server 4.1 SP6

Force updates for application loader tool IT policy rule

Description	This rule specifies whether a BlackBerry device user must update the application loader tool manually when an updated version is available and when the user updates the BlackBerry Device Software using BlackBerry Desktop Software.
Possible values	• Yes • No
Default value	• Yes
Exceptions	• BlackBerry Desktop Software 6.0
Minimum requirements	• BlackBerry Desktop Manager 5.0 SP1
Rule introduction	• BlackBerry Enterprise Server 5.0 SP2

Generate Encrypted Backup Files IT policy rule

Description	This rule specifies whether a BlackBerry device creates encrypted backup files. The device creates an encrypted backup file only when the BlackBerry Desktop Software is connected to your organization's network.
Possible values	• Yes • No
Default value	• No

Exceptions	• BlackBerry Desktop Software 6.0 • BlackBerry Enterprise Server for Novell GroupWise
Minimum requirements	• BlackBerry Desktop Manager 5.0
Rule introduction	• BlackBerry Enterprise Server 4.1 SP7

Override Check For Updates URL IT policy rule

Description	This rule specifies the destination web address for the Check for updates link in the BlackBerry Desktop Software.
Default value	• Null value
Exceptions	• BlackBerry Desktop Software 6.0
Minimum requirements	• BlackBerry Desktop Manager 4.5
Rule introduction	• BlackBerry Enterprise Server 4.1 SP5

Desktop Only policy group

Auto Backup Enabled IT policy rule

Description	This rule specifies whether the automatic backup option in the backup and restore tool of the BlackBerry Desktop Software or BlackBerry Web Desktop Manager is turned on.
Possible values	• Yes • No

Default value	• No
Exceptions	• BlackBerry Desktop Software 6.0 • BlackBerry Enterprise Server for Novell GroupWise only with the BlackBerry Web Desktop Manager
Minimum requirements	• BlackBerry Desktop Manager 3.5 or BlackBerry Web Desktop Manager 1.0
Rule introduction	• BlackBerry Enterprise Server 3.5 for Microsoft Exchange • BlackBerry Enterprise Server 4.0 for IBM Domino • BlackBerry Enterprise Server 4.0 for Novell GroupWise

Auto Backup Exclude Messages IT policy rule

Description	This rule specifies whether messages are excluded from an automatic backup.
Related rules	This rule affects the Auto Backup Include All IT policy rule. If you change this rule to Yes, you must configure the Auto Backup Include All IT policy rule to No.
Possible values	• Yes • No
Default value	• No
Exceptions	• BlackBerry Desktop Software 6.0 • BlackBerry Enterprise Server for Novell GroupWise only with the BlackBerry Web Desktop Manager
Minimum requirements	• BlackBerry Desktop Manager 3.5 or BlackBerry Web Desktop Manager 1.0
Rule introduction	• BlackBerry Enterprise Server 3.5 for Microsoft Exchange • BlackBerry Enterprise Server 4.0 for IBM Domino • BlackBerry Enterprise Server 4.0 for Novell GroupWise

Auto Backup Exclude Synchronization IT policy rule

Description	This rule specifies whether application data that is synchronized with desktop organizer applications is excluded from an automatic backup.
Related rules	This rule affects the Auto Backup Include All IT policy rule. If you change this rule to Yes, you must configure the Auto Backup Include All IT policy rule to No.
Possible values	• Yes • No
Default value	• No
Exceptions	• BlackBerry Desktop Software 6.0 • BlackBerry Enterprise Server for Novell GroupWise only with the BlackBerry Web Desktop Manager
Minimum requirements	• BlackBerry Desktop Manager 3.5 or BlackBerry Web Desktop Manager 1.0
Rule introduction	• BlackBerry Enterprise Server 3.5 for Microsoft Exchange • BlackBerry Enterprise Server 4.0 for IBM Domino • BlackBerry Enterprise Server 4.0 for Novell GroupWise

Auto Backup Frequency IT policy rule

Description	This rule specifies how often automatic backups occur.
Possible values	• 1 to 99 days
Default value	• 7 days
Exceptions	• BlackBerry Desktop Software 6.0

	• BlackBerry Enterprise Server for Novell GroupWise only with the BlackBerry Web Desktop Manager
Minimum requirements	• BlackBerry Desktop Manager 3.5 or BlackBerry Web Desktop Manager 1.0
Rule introduction	• BlackBerry Enterprise Server 3.5 for Microsoft Exchange • BlackBerry Enterprise Server 4.0 for IBM Domino • BlackBerry Enterprise Server 4.0 for Novell GroupWise

Auto Backup Include All IT policy rule

Description	This rule specifies whether all BlackBerry device data is included when an automatic backup occurs. By default, in the backup and restore tool options, the Backup all device application data option is selected.
Related rules	The Auto Backup Exclude Sync IT policy rule affects this rule. If you configure the Auto Backup Exclude Sync IT policy rule to Yes, change this rule to No. The Auto Backup Exclude Messages IT policy rule affects this rule. If you configure the Auto Backup Exclude Messages IT policy rule to Yes, change this rule to No.
Possible values	• Yes • No
Default value	• Yes
Exceptions	• BlackBerry Desktop Software 6.0 • BlackBerry Enterprise Server for Novell GroupWise only with the BlackBerry Web Desktop Manager
Minimum requirements	• BlackBerry Desktop Manager 3.5 or BlackBerry Web Desktop Manager 1.0
Rule introduction	• BlackBerry Enterprise Server 3.5 for Microsoft Exchange • BlackBerry Enterprise Server 4.0 for IBM Domino • BlackBerry Enterprise Server 4.0 for Novell GroupWise

Auto Signature IT policy rule

Description	This rule specifies the signature that is attached automatically to outgoing email messages. You can use this rule to add a disclaimer to the end of email messages that a BlackBerry device user sends from a BlackBerry device. This rule is obsolete in BlackBerry Enterprise Server 4.1 SP2 and later.
Default value	• Null value
Exceptions	• BlackBerry Desktop Software 6.0 • BlackBerry Enterprise Server for Novell GroupWise
Minimum requirements	• BlackBerry Desktop Manager 3.5
Rule introduction	• BlackBerry Enterprise Server for Microsoft Exchange 3.5 • BlackBerry Enterprise Server for IBM Domino 4.0

Disable Wireless Calendar IT policy rule

Description	This rule specifies whether a BlackBerry device user can use the wireless calendar synchronization option in the synchronization tool of the BlackBerry Desktop Software.
Possible values	• Yes • No
Default value	• No
Exceptions	• BlackBerry Desktop Software 6.0 and 6.01 • BlackBerry Enterprise Server for Novell GroupWise only with the BlackBerry Web Desktop Manager
Minimum requirements	• BlackBerry Desktop Manager 3.5 or BlackBerry Web Desktop Manager 1.0

Rule introduction	• BlackBerry Enterprise Server 3.5 for Microsoft Exchange • BlackBerry Enterprise Server 4.0 for IBM Domino • BlackBerry Enterprise Server 4.0 for Novell GroupWise

Do Not Save Sent Messages IT policy rule

Description	This rule specifies whether a BlackBerry device saves a copy of each email message that a BlackBerry device user sends in the sent messages folder on the user's computer.
Possible values	• Yes • No
Default value	• No
Exceptions	• BlackBerry Desktop Software 6.0 and 6.0.1 • BlackBerry Enterprise Server for Novell GroupWise only with the BlackBerry Web Desktop Manager
Minimum requirements	• BlackBerry Desktop Manager 3.5 or BlackBerry Web Desktop Manager 1.0
Rule introduction	• BlackBerry Enterprise Server 3.5 for Microsoft Exchange • BlackBerry Enterprise Server 4.0 for IBM Domino • BlackBerry Enterprise Server 4.0 for Novell GroupWise

Force Load Count IT policy rule

Description	This rule specifies the number of times that BlackBerry device users can decline to update the BlackBerry Device Software before they must update it. To turn off required updates to the BlackBerry Device Software, you can change the value for this rule to -1. To turn on required updates, you can change the value of this rule to 0 or higher. If you turn on required updates, the BlackBerry Desktop Software or BlackBerry Web Desktop Manager automatically checks for a new version of the software and prompts the user to update when the user logs in and connects a BlackBerry device to a computer.

Possible values	• -1 to 1000
Default value	• -1
Exceptions	• BlackBerry Desktop Software 6.0, 6.0.1, 7.0, and 7.1 • BlackBerry Enterprise Server for Novell GroupWise only with the BlackBerry Web Desktop Manager
Minimum requirements	• BlackBerry Desktop Manager 3.5 or BlackBerry Web Desktop Manager 1.0
Rule introduction	• BlackBerry Enterprise Server 3.5 for Microsoft Exchange • BlackBerry Enterprise Server 4.0 for IBM Domino • BlackBerry Enterprise Server 4.0 for Novell GroupWise

Force Load Message IT policy rule

Description	This rule specifies the message that appears when a BlackBerry device user is prompted to update the BlackBerry Device Software.
Related rules	The Force Load Count IT policy rule affects this rule. A BlackBerry device uses this rule only if you configure the Force Load Count IT policy rule to 0 or higher.
Default value	• Null value
Exceptions	• BlackBerry Desktop Software 6.0 and 6.0.1 • BlackBerry Enterprise Server for Novell GroupWise only with the BlackBerry Web Desktop Manager
Minimum requirements	• BlackBerry Desktop Manager 3.5 or BlackBerry Web Desktop Manager 1.0
Rule introduction	• BlackBerry Enterprise Server 3.5 for Microsoft Exchange • BlackBerry Enterprise Server 4.0 for IBM Domino • BlackBerry Enterprise Server 4.0 for Novell GroupWise

Forward Messages In Cradle IT policy rule

Description	This rule specifies whether a BlackBerry device receives email messages while it is connected to a computer.
Possible values	• Yes • No
Default value	• Yes
Exceptions	• BlackBerry Desktop Software 6.0 • BlackBerry Enterprise Server for Novell GroupWise
Minimum requirements	• BlackBerry Desktop Manager 3.5
Rule introduction	• BlackBerry Enterprise Server 3.5 for Microsoft Exchange • BlackBerry Enterprise Server 4.0 for IBM Domino

Message Conflict Mailbox Wins IT policy rule

Description	This rule specifies whether the email application on a computer takes precedence over a BlackBerry device when a conflict occurs during organizer data synchronization.
Possible values	• Yes • No
Default value	• Yes
Exceptions	• BlackBerry Desktop Software 6.0 and 6.0.1 • BlackBerry Enterprise Server for Novell GroupWise
Minimum requirements	• BlackBerry Desktop Manager 3.5

Rule introduction	• BlackBerry Enterprise Server 3.5 for Microsoft Exchange • BlackBerry Enterprise Server 4.0 for IBM Domino

Message Prompt IT policy rule

Description	This rule specifies the message that should appear when the BlackBerry Desktop Software starts.
Default value	• Null value
Exceptions	• BlackBerry Desktop Software 6.0 • BlackBerry Enterprise Server for Novell GroupWise
Minimum requirements	• BlackBerry Desktop Manager 3.5
Rule introduction	• BlackBerry Enterprise Server 3.5 for Microsoft Exchange • BlackBerry Enterprise Server 4.0 for IBM Domino

Show Application Loader IT policy rule

Description	This rule specifies whether the application loader tool appears in the BlackBerry Desktop Software and BlackBerry Web Desktop Manager. This rule is obsolete in BlackBerry Web Desktop Manager 5.0 and later.
Possible values	• Yes • No
Default value	• Yes
Exceptions	• BlackBerry Desktop Software 6.0 and 6.0.1 • BlackBerry Enterprise Server for Novell GroupWise only with BlackBerry Web Desktop Manager 1.0 or 1.0.1

Minimum requirements	• BlackBerry Desktop Manager 3.5 or BlackBerry Web Desktop Manager 1.0
Rule introduction	• BlackBerry Enterprise Server 3.5 for Microsoft Exchange • BlackBerry Enterprise Server 4.0 for IBM Domino

Show Web Link IT policy rule

Description	This rule specifies whether the link icon for the Internet appears in the BlackBerry Desktop Software.
Related rules	The Web Link URL IT policy rule affects this rule. The link icon appears only if you configure a default web address using the Web Link URL IT policy rule.
Possible values	• Yes • No
Default value	• No
Exceptions	• BlackBerry Desktop Software 6.0 and 6.0.1 • BlackBerry Enterprise Server for Novell GroupWise
Minimum requirements	• BlackBerry Desktop Manager 3.5
Rule introduction	• BlackBerry Enterprise Server 3.5 for Microsoft Exchange • BlackBerry Enterprise Server 4.0 for IBM Domino

Synchronize Messages Instead Of Importing IT policy rule

Description	This rule specifies whether a BlackBerry device can synchronize email messages and folders in the email application on a BlackBerry device user's computer and on the device instead of applying the changes to the device only.

Possible values	• Yes • No
Default value	• Yes
Exceptions	• BlackBerry Desktop Software 6.0 and 6.0.1 • BlackBerry Enterprise Server for Novell GroupWise
Minimum requirements	• BlackBerry Desktop Manager 3.5
Rule introduction	• BlackBerry Enterprise Server 3.5 for Microsoft Exchange • BlackBerry Enterprise Server 4.0 for IBM Domino

Web Link Label IT policy rule

Description	This rule specifies the name of the web link icon if it appears in the BlackBerry Desktop Software.
Related rules	The Show Web Link IT policy rule affects this rule. If you configure this rule, you must also change the Show Web Link IT policy rule to Yes so that the web link icon appears.
Default value	• Downloads
Exceptions	• BlackBerry Desktop Software 6.0 and 6.0.1 • BlackBerry Enterprise Server for Novell GroupWise
Minimum requirements	• BlackBerry Desktop Manager 3.5
Rule introduction	• BlackBerry Enterprise Server 3.5 for Microsoft Exchange • BlackBerry Enterprise Server 4.0 for IBM Domino

Web Link URL IT policy rule

Description	This rule specifies the web address for the web link icon, if it appears in the BlackBerry Desktop Software.
Related rules	The Show Web Link IT policy rule affects this rule. If you configure this rule, you must also configure the Show Web Link IT policy rule to Yes so that the web link icon appears.
Default value	• Null value
Exceptions	• BlackBerry Desktop Software 6.0 and 6.0.1 • BlackBerry Enterprise Server for Novell GroupWise
Minimum requirements	• BlackBerry Desktop Manager 3.5
Rule introduction	• BlackBerry Desktop Software 3.5 for Microsoft Exchange • BlackBerry Desktop Software 4.0 for IBM Domino

Device Configuration policy group

CCL Data Collection IT policy rule

Description	This rule specifies whether a BlackBerry device allows Context Collection Library (CCL) data collection across all apps. CCL allows apps to collect rich data related to app usage, and to carry out deep cross-application analysis. If you set this rule to Disallow, the device does not allow CCL data collection.
Possible values	• Allow • Disallow
Default value	• Allow

Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 5.0 SP4 • KB33177

Device IOT Application policy group

Device Diagnostic App Disable IT policy rule

Description	This rule specifies whether to prevent a BlackBerry device user from sending diagnostic reports from a BlackBerry device to the email and PIN addresses that you specify in the Set Diagnostic Report Email Address IT policy rule and Set Diagnostic Report PIN Address IT policy rule.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.2
Rule introduction	• BlackBerry Enterprise Server 4.0 SP6

Set Diagnostic Report Email Address IT policy rule

Description	This rule specifies one or more email addresses that should receive diagnostic reports. Separate multiple email addresses with a comma (,).
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.2

Rule introduction	• BlackBerry Enterprise Server 4.0 SP6

Set Diagnostic Report PIN Address IT policy rule

Description	This rule specifies one or more PINs that should receive diagnostic reports. Separate multiple PINs with a comma (,).
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.2
Rule introduction	• BlackBerry Enterprise Server 4.0 SP6

Device Only policy group

Allow BCC Recipients IT policy rule

Description	This rule specifies whether a BlackBerry device user can include recipients in the BCC field when the user composes email messages on a BlackBerry device.
Possible values	• Yes • No
Default value	• Yes
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise only with devices that are running BlackBerry Device Software 4.0 or later
Minimum requirements	• BlackBerry Device Software 3.6

Rule introduction	• BlackBerry Enterprise Server 3.5 for Microsoft Exchange • BlackBerry Enterprise Server 4.0 for IBM Domino • BlackBerry Enterprise Server 4.0 for Novell GroupWise

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. This rule does prevent the user from sending and receiving messages using BlackBerry Messenger. To prevent the user from sending and receiving messages using BlackBerry Messenger, use the Disable BlackBerry Messenger IT policy rule.
Related rules	The Firewall Block Incoming Messages IT policy rule affects this rule. To block incoming PIN messages, in the Security policy group, set the Firewall Block Incoming Messages IT policy rule to PIN Messages (Public) and PIN Messages (Corporate).
Possible values	• Yes • No
Default value	• Yes
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise only with devices that are running BlackBerry Device Software 4.0 or later
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server 3.5

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.

Related rules	The Firewall Block Incoming Messages IT policy rule affects this rule. To block incoming SMS text messages, in the Security policy group, configure the Firewall Block Incoming Messages IT policy rule.
Possible values	• Yes • No
Default value	• Yes
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise only with devices that are running BlackBerry Device Software 4.0 or later
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server 3.5

Default Browser Config UID IT policy rule

Description	This rule specifies the default browser that the BlackBerry device uses. Specify the UID of the service book for a browser to make it the default browser on the device. This rule is obsolete in BlackBerry Device Software 6.0.
Default value	• Null value
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise only with BlackBerry Device Software 4.0 or later
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server 3.5 for Microsoft Exchange • BlackBerry Enterprise Server 4.0 for IBM Domino • BlackBerry Enterprise Server 4.0 for Novell GroupWise

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 and Basic password security IT policy • Yes in all other IT policies
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise only with devices that are running BlackBerry Device Software 4.0 or later
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server 3.5

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

Exceptions	• BlackBerry Enterprise Server for Novell GroupWise only with devices that are running BlackBerry Device Software 4.0 or later
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server 3.5

Home Page Address IT policy rule

Description	This rule specifies the web address that the BlackBerry Browser uses as a home page. If you do not configure this rule, a BlackBerry device uses the default home page.
Default value	• Null value
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise only with devices running BlackBerry Device Software 4.0 or later
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server 3.5 for Microsoft Exchange • BlackBerry Enterprise Server 4.0 for IBM Domino • BlackBerry Enterprise Server 4.0 for Novell GroupWise

Home Page Address Is Read-Only IT policy rule

Description	This rule specifies whether a BlackBerry device user can change the BlackBerry Browser home page.
Possible values	• Yes • No
Default value	• No

Exceptions	• BlackBerry Enterprise Server for Novell GroupWise only with BlackBerry devices that are running BlackBerry Device Software 4.0 or later
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server 3.5 for Microsoft Exchange • BlackBerry Enterprise Server 4.0 for IBM Domino • BlackBerry Enterprise Server 4.0 for Novell GroupWise

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 • 60 days in the Basic Password Security IT policy • 30 days in all other preconfigured IT policies
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise only with devices running BlackBerry Device Software 4.0 or later
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server 3.5

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 • 30 minutes in the Basic Password Security IT policy • 10 minutes in all other preconfigured IT policies
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server 3.5

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
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise only with devices that are running BlackBerry Device Software 4.0 or later
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server 3.5

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 and Basic password security IT policy • At least 1 alpha and 1 numeric character in all other preconfigured IT policies
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise only with devices that are running BlackBerry Device Software 4.0 or later
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server 3.5

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 • Yes in all other preconfigured IT policies
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise only with devices running BlackBerry Device Software 4.0 or later
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server 3.5

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
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise only with BlackBerry devices that are running BlackBerry Device Software 4.0 or later
Minimum requirements	• BlackBerry Device Software 3.6

Rule introduction	• BlackBerry Enterprise Server 3.5

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 • No in all other preconfigured IT policies
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise only with devices that are running BlackBerry Device Software 4.0 or later
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server 3.5

Documents To Go policy group

Disable Creating and Editing Files using Documents To Go IT policy rule

Description	This rule specify whether a BlackBerry device user can create or edit a file using the Research In Motion version of the Documents To Go application on a BlackBerry device.
Related rules	The Disable Documents To Go IT policy rule affects this rule. If you set the Disable Documents To Go IT policy rule to Yes, the device ignores this rule.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry 7 • Research In Motion Documents To Go application 3.0.0
Rule introduction	• BlackBerry Enterprise Server 5.0 SP4

Disable Documents To Go IT policy rule

Description	This rule specifies whether a BlackBerry device user can open files or attachments using the Research In Motion or DataViz version of the Documents To Go application on a BlackBerry device.
Possible values	• Yes • No
Default value	• No

Minimum requirements	• BlackBerry Device Software 4.5 • RIM or DataViz Documents To Go application
Rule introduction	• BlackBerry Enterprise Server 4.1 SP5

Hide Documents To Go Communication Menus IT policy rule

Description	This rule specifies whether a BlackBerry device user can register the Documents To Go application with DataViz, check for software updates from DataViz, and use the premium edition of the DataVizDocuments To Go application on a BlackBerry device.
Related rules	The Disable Documents To Go IT policy rule affects this rule. If you configure the Disable Documents To Go IT policy rule to Yes, the device ignores this rule.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.5 • DataVizDocuments To Go application
Rule introduction	• BlackBerry Enterprise Server 4.1 SP5

Hide Documents To Go Premium Feature Menus IT policy rule

Description	This rule specifies whether to hide the premium features of the DataVizDocuments To Go application that are not available on a BlackBerry device that is running the standard edition of the Documents To Go application.

Related rules	The Disable Documents To Go IT policy rule affects this rule. If you configure the Disable Documents To Go IT policy rule to Yes, the device ignores this rule.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.5 • DataVizDocuments To Go application
Rule introduction	• BlackBerry Enterprise Server 4.1 SP5

Email Messaging policy group

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

Allow Auto Attachment Download IT policy rule

Description	This rule specifies whether a BlackBerry device automatically downloads supported attachments from email messages that it receives. This rule is obsolete in BlackBerry Enterprise Server 5.0 and later.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.2
Rule introduction	• BlackBerry Enterprise Server 4.0 SP6

Attachment Viewing IT policy rule

Description	This rule specifies whether a BlackBerry device user can view supported attachments in email messages and calendar entries. A BlackBerry device can use this rule if the BlackBerry Attachment Service is connected to the BlackBerry Enterprise Server using the BlackBerry Attachment Connector. Changing this rule to No does not prevent a user from downloading or viewing native attachments on a device.
Possible values	• Yes • No
Default value	• Yes
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise only with devices that are running BlackBerry Device Software 4.0 or later
Minimum requirements	• BlackBerry Device Software 3.7 • BlackBerry Device Software 5.0 or later for calendar attachments • BlackBerry Enterprise Server 5.0 or later for calendar attachments
Rule introduction	• BlackBerry Enterprise Server 3.6.1 for Microsoft Exchange • BlackBerry Enterprise Server 4.0 for IBM Domino • BlackBerry Enterprise Server 4.0 for Novell GroupWise

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 5.0

Disable Form Submission IT policy rule

Description	This rule specifies whether a BlackBerry device user can send email messages that include embedded forms.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.5
Rule introduction	• BlackBerry Enterprise Server 4.1 SP5

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 4.1 SP5

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 Domino encrypted email messages using a BlackBerry device. By default, a user that has a device that supports for reading IBM 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 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 4.1 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 4.1 SP5

Enable Wireless Message Reconciliation IT policy rule

Description	This rule specifies whether a BlackBerry device supports wireless email reconciliation. When a BlackBerry device user moves or deletes email messages using a device or the email application on a computer, or marks email messages as opened or unopened, the BlackBerry Messaging Agent reconciles the changes over the wireless network.
Possible values	• Yes • No
Default value	• Yes
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise only with devices that are running BlackBerry Device Software 4.0 or later
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server 3.6 for Microsoft Exchange • BlackBerry Enterprise Server 4.0 for IBM Domino • BlackBerry Enterprise Server 4.0 for Novell GroupWise

Inline Content Requests IT policy rule

Description	This rule specifies whether a BlackBerry device user can send email messages that include inline content and view inline content automatically in email messages using a BlackBerry device. If you set this rule to Manual Only, a user must request inline content in email messages manually.

Possible values	• Manual only • Automatic allowed • Disabled
Default value	• Automatic allowed
Minimum requirements	• BlackBerry Device Software 4.5
Rule introduction	• BlackBerry Enterprise Server 4.1 SP5

Keep Message Duration IT policy rule

Description	This rule specifies the maximum amount of time that a BlackBerry device stores messages for. Configure this rule to 0 or -1 to store messages on a device indefinitely. The device may take up to 24 hours longer than the amount of time that you specify in this rule to remove messages because most devices begin the cycle to remove email messages 24 hours after the device resets.
Possible values	• -1 to 180 days
Default value	• -1
Minimum requirements	• BlackBerry Device Software 4.2
Rule introduction	• BlackBerry Enterprise Server 4.0 SP6

Keep Saved Message Duration IT policy rule

Description	This rule specifies the maximum amount of time that a BlackBerry device stores saved messages for. Configure this rule to 0 or -1 to store saved messages on a device indefinitely. With a device that is running BlackBerry Device Software 4.5 or later, you can set this rule to -2 to delete saved messages and prevent a user from saving messages on the device.

	The device may take up to 24 hours longer than the amount of time that you specify in this rule to remove messages because most devices begin the cycle to remove messages 24 hours after the device resets.
Possible values	• -2 to 180 days
Default value	• -1
Minimum requirements	• BlackBerry Device Software 4.2
Rule introduction	• BlackBerry Enterprise Server 4.0 SP6

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.
Related rules	In BlackBerry Enterprise Server 5.0 or later, this rule interacts with the Maximum single attachment upload size (KB) field in the BlackBerry Administration Service. In BlackBerry Enterprise Server versions earlier than 5.0, this rule interacts with the Maximum Upload Attachment Size field in the BlackBerry Manager. If you configure these fields, the BlackBerry Enterprise Server sends the values to the device using service books. The device cannot send an attachment that exceeds the size that you specify in the fields.
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 4.0 SP6

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.
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 4.0 SP6

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.
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 4.1 SP5

Notes Native Encryption Password Timeout IT policy rule

Description	This rule specifies the maximum length of time that a BlackBerry device stores the IBM 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 4.1 SP5

Prepend Disclaimer IT policy rule

Description	This rule specifies the disclaimer that appears at the beginning of all email messages that a BlackBerry device user sends from a BlackBerry device.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.1.2
Rule introduction	• BlackBerry Enterprise Server 4.0 SP5

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

Enterprise Voice Client policy group

The BlackBerry Mobile Voice System only supports this IT policy group in BlackBerry MVS 4.5 and 4.6.

Disable DTMF Fallback IT policy rule

Description	This rule specifies whether a BlackBerry device can use DTMF for outgoing calls if the device does not have adequate wireless coverage to place outgoing calls using the gateway message envelope protocol. DTMF uses weaker authentication than the gateway message envelope protocol.
Possible values	• Yes

	• No
Default value	• No
Minimum requirements	• BlackBerry Mobile Voice System 4.5 or 4.6
Rule introduction	• BlackBerry Enterprise Server 4.1 SP4 • KB15124

Disable Enterprise Voice Client IT policy rule

Description	This rule specifies whether enterprise voice is available on a BlackBerry device.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Mobile Voice System 4.5 or 4.6
Rule introduction	• BlackBerry Enterprise Server 4.1 SP4 • KB15124

Lock Outgoing Line IT policy rule

Description	This rule specifies whether to prevent using the enterprise voice number for outgoing calls.
Possible values	• Yes • No
Default value	• No

Minimum requirements	• BlackBerry Mobile Voice System 4.5 or 4.6
Rule introduction	• BlackBerry Enterprise Server 4.1 SP4 • KB15124

Reject Non-Enterprise Voice Calls IT policy rule

Description	This rule specifies whether the BlackBerry device accepts incoming calls only if they are sent through the BlackBerry Enterprise Server. This rule is obsolete in BlackBerry Enterprise Server 4.1 SP4 and later.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Mobile Voice System 4.5 or 4.6
Rule introduction	• BlackBerry Enterprise Server 4.1 SP4 • KB15124

External Display policy group

Display Notification Details IT policy rule

Description	This rule specifies when notifications appear on the external display of BlackBerry Pearl Flip Series smartphones.
Possible values	• Never

	• Always • Only when unlocked
Default value	• Always
Minimum requirements	• BlackBerry Pearl Flip Series smartphone • BlackBerry Device Software 4.6
Rule introduction	• BlackBerry Enterprise Server 4.1 SP6

Include Message Text in Notification Details IT policy rule

Description	This rule specifies whether preview text for notifications appears on the external display of BlackBerry Pearl Flip Series smartphones.
Related rules	The Display Notification Details IT policy rule affects this rule. A BlackBerry device uses this rule only if the Display Notification Details IT policy rule is configured to Only when unlocked or Always.
Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry Pearl Flip Series smartphone • BlackBerry Device Software 4.6
Rule introduction	• BlackBerry Enterprise Server 4.1 SP6

Firewall policy group

Restrict Incoming Cellular Calls IT policy rule

Description	This rule specifies whether the firewall on a BlackBerry device blocks incoming calls. This rule does not affect emergency calls. A BlackBerry device user must subscribe to caller ID to use this rule. Separate multiple values with a semi-colon (;). To block all incoming calls, type **r**. To block a phone number, append **r** to the phone number. For example, type **+15195551234r** to block calls from 519-555-1234. To block phone numbers that use a dialing pattern, append **r** to the dialing pattern. For example, type **011...r** to block calls from phone numbers that use the dialing pattern *011xxxxxxxxx*. To block all phone numbers except for the phone numbers that you allow, type the phone number followed by **;r**. For example, type **+15195551234;r** to allow calls from 519-555-1234 only. To block all phone numbers except for phone numbers that follow a dialing pattern that you allow, type the dialing pattern followed by **;r**. For example, type **011...;r** to allow calls from phone numbers that use the dialing pattern *011xxxxxxxxx* only.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.3
Rule introduction	• BlackBerry Enterprise Server 4.1 SP5

Restrict Outgoing Cellular Calls IT policy rule

Description	This rule specifies whether a BlackBerry device firewall blocks outgoing calls. This rule does not affect emergency calls. A BlackBerry device user must subscribe to caller ID to use this rule. Separate Type one or more fixed dialing patterns (for example, specific dialing numbers or a set of dialing numbers that have the same prefix) separated by a semi-colon (;). To block all outgoing calls, type **r**.

	To block a phone number, append **r** to the phone number. For example, type **+15195551234r** to block calls to 519-555-1234. To block phone numbers that use a dialing pattern, append **r** to the dialing pattern. For example, type **011...r** to block calls to phone numbers that use the dialing pattern *011xxxxxxxxx*. To block all phone numbers except for the phone numbers that you allow, type the phone number followed by **;r**. For example, type **+15195551234;r** to allow calls to 519-555-1234 only. To block all phone numbers except for phone numbers that follow a dialing pattern that you allow, type the dialing pattern followed by **;r**. For example, type **011...;r** to allow calls to phone numbers that use the dialing pattern *011xxxxxxxxx* only.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.3
Rule introduction	• BlackBerry Enterprise Server 4.1 SP5

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
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise only with devices that are running BlackBerry Device Software 4.0 or later
Minimum requirements	• BlackBerry Device Software 3.6

Rule introduction	• BlackBerry Enterprise Server 3.5

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
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise only with devices that are running BlackBerry Device Software 4.0 or later
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server 3.5

Instant Messaging policy group

Disable Address Book Lookup for Enterprise Messenger IT policy rule

Description	This rule specifies whether a BlackBerry device user can add a contact to a BlackBerry device by searching the contact list if the user uses a collaboration client (such as the BlackBerry Client for use with Microsoft Office Communications Server 2007). The contact-list search can return an email address that the user cannot use to add a contact because the search does not return the correct SIP address.

Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.2
Rule introduction	• BlackBerry Enterprise Server 4.1 SP6

Disable Automatic Login IT policy rule

Description	This rule specifies whether a BlackBerry device user can permit collaboration clients that were previously logged in on a BlackBerry device to log back in automatically after the device restarts or enters a wireless coverage area again.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.5
Rule introduction	• BlackBerry Enterprise Server 5.0 SP1

Disable BBM Connected App Features IT policy rule

Description	This rule specifies whether a BlackBerry device user can use BBM connected apps with BlackBerry Messenger on the device. If you set this rule to Yes, BBM connected apps cannot be integrated with BlackBerry Messenger on the device.
Possible values	• Yes • No

Default value	• No
Minimum requirements	• BlackBerry Device Software 5.0 • BlackBerry Messenger 6.0
Rule introduction	• BlackBerry Enterprise Server 5.0 SP4

Disable Broadcast Messages IT policy rule

Description	This rule specifies whether a BlackBerry device user can send email messages or PIN messages to multiple recipients from a BlackBerry device.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.5
Rule introduction	• BlackBerry Enterprise Server 5.0 SP1

Disable Emailing Conversation IT policy rule

Description	This rule specifies whether a BlackBerry device user can send an instant-messaging conversation in an email message from a BlackBerry device.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.1

Rule introduction	• BlackBerry Enterprise Server 4.1 SP6

Disable Emoticons IT policy rule

Description	This rule specifies whether the collaboration client on a BlackBerry device prevents the use and display of emoticons.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.5
Rule introduction	• BlackBerry Enterprise Server 5.0 SP1

Disable Offline Messaging for Enterprise Messenger IT policy rule

Description	This rule specifies whether a BlackBerry device user can send a message to an offline contact using the collaboration client on a BlackBerry device.
Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry Device Software 4.5
Rule introduction	• BlackBerry Enterprise Server 5.0 SP1

Disable Saving Conversation IT policy rule

Description	This rule specifies whether a BlackBerry device user can save an instant-messaging conversation to a BlackBerry device or media card.
Possible value	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.2
Rule introduction	• BlackBerry Enterprise Server 4.1 SP6

Disallow File Transfer Types IT policy rule

Description	This rule specifies the types of files that a BlackBerry device user cannot send using an instant-messaging application on a BlackBerry device. Specify the extensions of the restricted file types in a comma-delimited format (for example, bat, exe, mp3) to prevent a user from sending specific file types. Type an asterisk (*) to prevent a user from sending any file type.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.2
Rule introduction	• BlackBerry Enterprise Server 4.1 SP6

Maximum File Transfer Size (MB) IT policy rule

Description	This rule specifies the maximum size of files that a collaboration client can send to an instant messaging server.

Possible values	• 0 to 6 MB
Default value	• 6 MB
Minimum requirements	• BlackBerry Device Software 4.5
Rule introduction	• BlackBerry Enterprise Server 5.0 SP1

Location Based Services policy group

Allow Geolocation Service IT policy rule

Description	This rule specifies whether a BlackBerry device can use the geolocation service to identify the geographic location of a BlackBerry device user. The geolocation service is available only on devices that have internal GPS capability.
Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server 5.0

Disable BlackBerry Maps IT policy rule

Description	This rule specifies whether the BlackBerry Maps feature is turned on.

Possible values	• Yes • No
Default value	• No
Rule introduction	• BlackBerry Enterprise Server 4.0 SP6

Enable Enterprise Location Tracking IT policy rule

Description	This rule specifies whether a BlackBerry device can use the GPS feature to report its location to the BlackBerry Enterprise Server at regular intervals. A BlackBerry device user must click Yes when prompted to permit location tracking on a device.
Related rules	The Enterprise Location Tracking Interval IT policy rule affects this rule. Use the Enterprise Location Tracking Interval IT policy rule to change the interval that a device reports its location to the BlackBerry Enterprise Server.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.2.2
Rule introduction	• BlackBerry Enterprise Server 4.1 SP3

Enterprise Location Tracking Interval IT policy rule

Description	This rule specifies the length of time between location reports that a BlackBerry device sends to the BlackBerry Enterprise Server.
Possible values	• 15 to 60 minutes

Default value	• 15 minutes
Minimum requirements	• BlackBerry Device Software 4.2.2
Rule introduction	• BlackBerry Enterprise Server 4.1 SP3

Enterprise Location Tracking User Prompt Message IT policy rule

Description	This rule specifies the message that a BlackBerry device displays to notify a BlackBerry device user that the BlackBerry Enterprise Server is tracking the location of the device.
Default value	• Your location is now being tracked at the server.
Minimum requirements	• BlackBerry Device Software 4.2.2
Rule introduction	• BlackBerry Enterprise Server 4.1 SP3

MDS Integration Service policy group

The rules in the MDS Integration Service policy group are obsolete in BlackBerry Enterprise Server 5.0 SP3 and later.

Allow Access to Multiple Domains IT policy rule

Description	This rule specifies whether to permit a BlackBerry device user to install a BlackBerry MDS Runtime Application that uses multiple web services on a BlackBerry device. This rule is obsolete in BlackBerry Enterprise Server 5.0 SP3 and later.
Possible values	• Yes

	• No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.5
Rule introduction	• BlackBerry Enterprise Server 5.0

Allow Discovery By User IT policy rule

Description	This rule specifies whether to prevent a BlackBerry device user from searching for and installing BlackBerry MDS Runtime applications on a BlackBerry device. This rule is obsolete in BlackBerry Enterprise Server 5.0 SP3 and later.
Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry Device Software 4.5
Rule introduction	• BlackBerry Enterprise Server 5.0

Disable Activation With Public BlackBerry MDS Integration Service IT policy rule

Description	This rule specifies whether to prevent a BlackBerry device user from connecting to the public BlackBerry MDS Integration Service. This rule is obsolete in BlackBerry Enterprise Server 4.0 SP6 and later.
Possible values	• Yes

	• No
Default value	• No
Rule introduction	• BlackBerry Enterprise Server 4.0 SP6

Disable MDS Runtime IT policy rule

Description	This rule specifies whether the BlackBerry MDS Runtime is available on a BlackBerry device. This rule is obsolete in BlackBerry Enterprise Server 5.0 SP3 and later.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0 SP6

Disable User-Initiated Activation With Public BlackBerry MDS Integration Service IT policy rule

Description	This rule specifies whether to prevent a BlackBerry device user from connecting to the BlackBerry MDS Integration Service. This rule is obsolete in BlackBerry Enterprise Server 5.0 SP3 and later.
Possible values	• Yes • No
Default value	• No

Minimum requirements	• BlackBerry Device Software 4.2
Rule introduction	• BlackBerry Enterprise Server 4.0 SP6

Enable Access to Device Data for MDS Runtime 4.3.0 and earlier IT policy rule

Description	This rule specifies whether BlackBerry MDS Runtime 4.3.0 and earlier can access the organizer data, interprocess communication, and phone on a BlackBerry device. This rule is obsolete in BlackBerry Enterprise Server 5.0 SP3 and later.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.1.0
Rule introduction	• BlackBerry Enterprise Server 5.0

Lowest BlackBerry MDS Integration Service Security Version Allowed IT policy rule

Description	This rule specifies which versions of the BlackBerry MDS Integration Service that a BlackBerry device can connect to. Change this rule to 1 to permit a BlackBerry device that is running BlackBerry MDS Runtime 1.1 or later to connect to all versions of the BlackBerry MDS Integration Service. Change this rule to 2 to permit a device that is running BlackBerry MDS Runtime 1.1 or later to connect to BlackBerry MDS Integration Service 4.1 SP2 or later only. This rule is obsolete in BlackBerry Enterprise Server 5.0 SP3 and later.
Possible values	• 1 to 65,535

Default value	• 1
Minimum requirements	• BlackBerry Device Software 4.2
Rule introduction	• BlackBerry Enterprise Server 4.0 SP6

Queue Limit for Inbound Application Messages IT policy rule

Description	This rule specifies the maximum number of incoming application messages from BlackBerry MDS Runtime that a BlackBerry device can queue. This rule is obsolete in BlackBerry Enterprise Server 5.0 SP3 and later.
Possible values	• 0 to 50 messages
Default value	• 8 messages
Minimum requirements	• BlackBerry Device Software 4.5
Rule introduction	• BlackBerry Enterprise Server 5.0

Queue Limit for Outbound Application Messages IT policy rule

Description	This rule specifies the number of outgoing application messages from the BlackBerry MDS Runtime that a BlackBerry device can queue. This rule is obsolete in BlackBerry Enterprise Server 5.0 SP3 and later.
Possible values	• 0 to 50 messages

Default value	• 16 messages
Minimum requirements	• BlackBerry Device Software 4.5
Rule introduction	• BlackBerry Enterprise Server 5.0

Verify BlackBerry MDS Integration Service Certificate IT policy rule

Description	This rule specifies whether the BlackBerry MDS Runtime verifies the BlackBerry MDS Integration Service certificate. This rule is obsolete in BlackBerry Enterprise Server 5.0 SP3 and later.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.2
Rule introduction	• BlackBerry Enterprise Server 4.0 SP6

Media Server policy group

Media Server IT policy rule

Description	This rule specifies whether a BlackBerry device user can use the media server on the device to share media files from the device with supported devices that are UPnP compatible or DLNA Certified.

Possible values	• Allow • Disallow
Default value	• Allow
Minimum requirements	• BlackBerry 7.1 (bundle 1247)
Rule introduction	• BlackBerry Enterprise Server 5.0 SP4 • KB29510

Memory Cleaner policy group

For more information about cleaning the BlackBerry device memory, see the *BlackBerry Enterprise Solution Security Technical Overview*.

Force Memory Clean When Closed IT policy rule

Description	This rule specifies whether a BlackBerry Pearl Flip Series smartphone run the memory cleaner application when the device is closed.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Pearl Flip Series smartphone • BlackBerry Device Software 4.6
Rule introduction	• BlackBerry Enterprise Server 4.1 SP6

Force Memory Clean When Holstered IT policy rule

Description	This rule specifies whether a BlackBerry device runs the memory cleaner application when the device is in the holster.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server 4.0 SP3

Force Memory Clean When Idle IT policy rule

Description	This rule specifies whether a BlackBerry device runs the memory cleaner application during periods of BlackBerry device user inactivity.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server 4.0 SP3

Memory Cleaner Maximum Idle Time IT policy rule

Description	This rule specifies the maximum amount of time that a BlackBerry device can be inactive before the device runs the memory cleaner application.
Related rules	The Force Memory Clean When Idle IT policy rule affects this rule. A device uses this rule only if you configure the Force Memory Clean When Idle IT policy rule to Yes.
Possible values	• 1 to 60 minutes
Default value	• 60 minutes
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server 4.0 SP3

NFC policy group

Allow NFC Card Emulation Mode IT policy rule

Description	This rule specifies whether a BlackBerry device can emulate an NFC tag or an NFC card. If you set this rule to Yes, the device acts as an NFC tag, which can be used as a contactless smart card (for example, for contactless payments and e-ticketing).
Related rules	The NFC Features IT policy rule affects this rule. The device uses this rule only if you set the NFC Features IT policy rule to Allow.
Possible values	• Yes • No
Default value	• Yes

Minimum requirements	• BlackBerry 7
Rule introduction	• BlackBerry Enterprise Server 5.0 SP4 • KB28284

Allow NFC Peer to Peer Device Communication Mode IT policy rule

Description	This rule specifies whether a BlackBerry device can send or receive data using NFC peer-to-peer communication. In peer-to-peer device communication mode, two NFC devices can exchange data (for example Bluetooth set-up parameters, virtual business cards, or digital photos).
Related rules	The NFC Features IT policy rule affects this rule. The device uses this rule only if you set the NFC Features IT policy rule to Allow.
Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry 7
Rule introduction	• BlackBerry Enterprise Server 5.0 SP4 • KB28284

Allow NFC Tag Reader/Writer Mode IT policy rule

Description	This rule specifies whether a BlackBerry device can read and write NFC tags and NFC cards.
Related rules	The NFC Features IT policy rule affects this rule. The device uses this rule only if you set the NFC Features IT policy rule to Allow.
Possible values	• Yes

	• No
Default value	• Yes
Minimum requirements	• BlackBerry 7
Rule introduction	• BlackBerry Enterprise Server 5.0 SP4 • KB28284

NFC Features IT policy rule

Description	This rule specifies whether a BlackBerry device can use NFC features.
Possible values	• Allow • Disallow
Default value	• Allow
Minimum requirements	• BlackBerry 7
Rule introduction	• BlackBerry Enterprise Server 5.0 SP4 • KB28284

On-Device Help policy group

On-Device Help Group Label IT policy rule

Description	This rule specifies a label to use for a group of links in the help on a BlackBerry device.

Related rules	The On-Device Help Links IT policy rule affects this rule. Configure a group label if you specify multiple links using the On-Device Help Links IT policy rule.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.1
Rule introduction	• BlackBerry Enterprise Server 4.0 SP3

On-Device Help Links IT policy rule

Description	This rule specifies links that you add to the index page of the help on a BlackBerry device. Specify links using the following format: *<uri1|label1|>...<|urix|labelx>* .
Related rules	This rule affects the On-Device Help Group Label IT policy rule. If you specify multiple links, you should also configure a label in the On-Device Help Group Label IT policy rule.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.1
Rule introduction	• BlackBerry Enterprise Server 4.0 SP3

On-Device Diagnostics policy group

Application Resource Monitor IT policy rule

Description	This rule specifies whether a BlackBerry device user can use the Application Resource Monitor. If you set this rule to Allow, users can turn on the Application Resource Monitor. If you set this rule to Disallow, the Application Resource Monitor is disabled on the BlackBerry device.

Possible values	• Allow • Disallow
Default value	• Allow
Minimum requirements	• BlackBerry 7.1
Rule introduction	• BlackBerry Enterprise Server 5.0 SP4

Battery Saving Mode IT policy rule

Description	This rule specifies whether a BlackBerry device can run in battery saving mode. If you set this rule to Disallow, battery saving mode is not available on the device.
Possible values	• Allow • Disallow
Default value	• Allow
Minimum requirements	• BlackBerry 7.1 (bundle 1582)
Rule introduction	• BlackBerry Enterprise Server 5.0 SP4 • KB29510

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.
Possible values	• AES (256-bit) • AES (192-bit) • AES (128-bit) • CAST (128-bit) • Triple DES
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise
Minimum requirements	• PGP Support Package for BlackBerry smartphones 4.1 • BlackBerry Device Software 4.1
Rule introduction	• BlackBerry Enterprise Server 4.0 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.
Possible values	• None • Manual • Automatic
Default value	• Automatic

Minimum requirements	• BlackBerry Device Software 4.5
Rule introduction	• BlackBerry Enterprise Server 4.1 SP5

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.
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 4.1 SP6

PGP Blind Copy Address IT policy rule

Description	This rule specifies an email address that is added as a BCC recipient to all encrypted PGP messages that a BlackBerry device sends.
Default value	• Null value
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise
Minimum requirements	• PGP Support Package for BlackBerry smartphones 4.1 • BlackBerry Device Software 4.1

Rule introduction	• BlackBerry Enterprise Server 4.0 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 Symantec Encryption Management Server.
Possible values	• Yes • No
Default value	• No
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise
Minimum requirements	• PGP Support Package for BlackBerry smartphones 4.1 • BlackBerry Device Software 4.1
Rule introduction	• BlackBerry Enterprise Server 4.0 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 Symantec Encryption Management Server.
Possible values	• Yes • No
Default value	• No
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise

Minimum requirements	• PGP Support Package for BlackBerry smartphones 4.1 • BlackBerry Device Software 4.1
Rule introduction	• BlackBerry Enterprise Server 4.0 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.
Related rules	This rule affects the Disable Weak Certificate Use IT policy rule. Configure the Disable Weak Certificate Use IT policy rule to Yes to prevent a BlackBerry device user from sending email messages using certificates that have corresponding weak public keys.
Possible values	• 512 to 4096 bits
Default value	• 1024 bits
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise
Minimum requirements	• PGP Support Package for BlackBerry smartphones 4.1 • BlackBerry Device Software 4.1
Rule introduction	• BlackBerry Enterprise Server 4.0 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.
Related rules	This rule affects the Disable Weak Certificate Use IT policy rule. Configure the Disable Weak Certificate Use IT policy rule to Yes to prevent a BlackBerry device user from sending email messages using certificates that have corresponding weak public keys.

Possible values	• 512 to 1024 bits
Default value	• 1024 bits
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise
Minimum requirements	• PGP Support Package for BlackBerry smartphones 4.1 • BlackBerry Device Software 4.1
Rule introduction	• BlackBerry Enterprise Server 4.0 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.
Related rules	This rule affects the Disable Weak Certificate Use IT policy rule. Configure the Disable Weak Certificate Use IT policy rule to Yes to prevent BlackBerry device users from sending email messages using certificates that have corresponding weak public keys.
Possible values	• 512 to 4096 bits
Default value	• 1024 bits
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise
Minimum requirements	• PGP Support Package for BlackBerry smartphones 4.1 • BlackBerry Device Software 4.1
Rule introduction	• BlackBerry Enterprise Server 4.0 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.
Possible values	• Automatic • Manual • None
Default value	• Manual
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server 5.0 SP1

PGP Universal Enrollment Method IT policy rule

Description	This rule specifies the method that a BlackBerry device user must use to enroll with the Symantec Encryption Management Server on a BlackBerry device. The user must submit the enrollment information to the Symantec Encryption Management Server before the user sends and receives PGP protected messages on the device.
Possible values	• Domain username/password enrollment • Email-based enrolment
Default value	• Email-based enrollment
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise
Minimum requirements	• PGP Support Package for BlackBerry smartphones 4.1 • BlackBerry Device Software 4.1

Rule introduction	• BlackBerry Enterprise Server 4.0 SP2

PGP Universal Policy Cache Timeout IT policy rule

Description	This rule specifies the length of time that a BlackBerry device caches the Symantec Encryption Management Server address.
Possible values	• 4 to 48 hours
Default value	• 24 hours
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise
Minimum requirements	• PGP Support Package for BlackBerry smartphones 4.1 • BlackBerry Device Software 4.1
Rule introduction	• BlackBerry Enterprise Server 4.0 SP2

Symantec Encryption Management Server Address IT policy rule

Description	This rule specifies the address of your organization's Symantec Encryption Management Server. The Symantec Encryption Management Server applies email policies that the Symantec Encryption Management Server administrator configures. Configure this rule to require that the BlackBerry device user registers with the Symantec Encryption Management 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
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise

Minimum requirements	• PGP Support Package for BlackBerry smartphones 4.1 • BlackBerry Device Software 4.1
Rule introduction	• BlackBerry Enterprise Server 4.0 SP2

PIM Synchronization policy group

Disable Address Wireless Synchronization IT policy rule

Description	This rule specifies whether wireless data synchronization for the address book on a BlackBerry device is turned off.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0

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 The device does not report the time that the IT policy updated, model name, BlackBerry Device Software version, phone number, or SIM information to the BlackBerry Enterprise Server, although you can verify this information on the device. If you apply this rule, the user account name no longer appears in the SyncDeviceMgmtSummary table in the BlackBerry Configuration Database.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0

Disable BlackBerry Messenger Wireless Synchronization IT policy rule

Description	This rule specifies whether wireless synchronization of the message database for the BlackBerry Messenger is turned off. When you change this rule, the BlackBerry Messenger logs all instant-message text in unencrypted format in the log file that you specify. You must verify that the log file is in a location that your organization's security policies restrict access to.
Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry Device Software 4.5 • BlackBerry Messenger 5.0

Rule introduction	• BlackBerry Enterprise Server 5.0 SP1

Disable Calendar Wireless Synchronization IT policy rule

Description	This rule specifies whether wireless data synchronization for the calendar is turned off.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0

Disable Enterprise Activation Progress IT policy rule

Description	This rule specifies whether the Home screen on the BlackBerry device displays enterprise-activation progress.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.2
Rule introduction	• BlackBerry Enterprise Server 4.0 SP6

Disable Memopad Wireless Synchronization IT policy rule

Description	This rule specifies whether wireless data synchronization for memos is turned off.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0

Disable Phone Call Log Wireless Synchronization IT policy rule

Description	This rule specifies whether wireless data synchronization for call logs is turned off.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.1
Rule introduction	• BlackBerry Enterprise Server 4.0 SP6

Disable PIN Messages Wireless Synchronization IT policy rule

Description	This rule specifies whether wireless data synchronization for PIN messages is turned off.
Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry Device Software 4.1
Rule introduction	• BlackBerry Enterprise Server 4.0 SP6

Disable SMS Messages Wireless Synchronization IT policy rule

Description	This rule specifies whether wireless data synchronization for SMS text messages is turned off.
Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry Device Software 4.1
Rule introduction	• BlackBerry Enterprise Server 4.0 SP6

Disable Task Wireless Synchronization IT policy rule

Description	This rule specifies whether wireless data synchronization for tasks is turned off.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0

Disable Wireless Bulk Loads IT policy rule

Description	This rule specifies whether wireless data synchronization is turned off during the BlackBerry device activation or as part of a backup and restore process. The device must be physically connected to a computer before the data transfer starts. If a device is disconnected from the computer during the initial data transfer, the BlackBerry Desktop Software sends the remaining data over the wireless network.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0

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*.

Duress Notification Address IT policy rule

Description	This rule specifies the email address that is notified when BlackBerry device users type a BlackBerry device password under duress. Users can indicate that they are unlocking their devices against their will by moving the first character of the password to the end. For example, if a device password is example, the duress password is xamplee. Configure this rule to permit users to notify you that a device might have been stolen. Instruct users how to use the duress password feature. If you configure this rule, the maximum number times that a user can try a password is reduced by half. Each time a user types a password to unlock a device, the device must verify whether the password is either the correct password or the duress password. To prevent an unlocked device that was stolen from receiving a response to the duress notification, the email address that you specify should be active and you should not configure an out-of-office reply for it.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0

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 4.0 SP2

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.
Possible values	• 0 to 15 passwords
Default values	• 0 in the Default and Basic password security IT policies • 6 in all other preconfigured IT policies
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise only with devices that are running BlackBerry Device Software 4.0 or later
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server 3.6

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 4.0

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

Exceptions	• BlackBerry Enterprise Server for Novell GroupWise only with devices running BlackBerry Device Software 4.0 and later
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server 3.6

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
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise only with devices running BlackBerry Device Software 4.0 and later
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server 3.5

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
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise only with devices running BlackBerry Device Software 4.0 or later
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server 3.6

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).
Possible values	• Yes • No
Default value	• No

Minimum requirements	• BlackBerry 6
Rule introduction	• BlackBerry Enterprise Server 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.
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 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).

Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry 6
Rule introduction	• BlackBerry Enterprise Server 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 5.0 SP3

Phone policy group

Enable Auto-Answer Incoming Call User Option IT policy rule

Description	This rule specifies whether a BlackBerry device user can set the Auto Answer setting on the device to the After 5 seconds option. If you set this rule to No, the user cannot configure the device to answer incoming calls automatically after 5 seconds.
Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry 7
Rule introduction	• BlackBerry Enterprise Server 5.0 SP4 • KB28284

Disable Enhanced Caller ID Information Lookup IT policy rule

Description	This rule specifies whether a BlackBerry device can send caller ID information to a server that is external to your organization that provides enhanced caller ID information, such as name, company, location, and picture.
Possible values	• Yes • No

Default value	• No
Minimum requirements	• BlackBerry 7.1
Rule introduction	• BlackBerry Enterprise Server 5.0 SP4

Outgoing Call Redirection IT policy rule

Description	This rule specifies how a BlackBerry device redirects outgoing calls automatically. When you set this rule, a BlackBerry device user can place a call to a phone number and the device redirects the call to another phone number automatically. For example, you can use this rule to forward a 411 call to your organization's help desk or a long-distance number to a toll-free number. This rule applies to all outgoing calls. To forward outgoing calls on devices, you must configure the value of this rule using the remap0<*search_prefix*>,<*replace_prefix*>,<*min_count*>,<*max_count*> format. • <*search_prefix*> is the prefix in the phone number that the device must match or replace • <*replace_prefix*> is the new prefix or new phone number that the device must use • <*min_count*> is the minimum number of digits that must follow the prefix for the match between the phone number and <*search_prefix*> to be valid • <*max_count*> is the maximum number of digits that must follow the prefix for the match between the phone number and <*search_prefix*> to be valid Valid characters for <*search_prefix*> and <*replace_prefix*> are numbers zero to nine (0 to 9), the asterisk (*), the number symbol (#), and the plus sign (+), where the plus sign is the international code placeholder. The value of <*min_count*> cannot exceed <*max_count*>. Consider the following examples: • To configure a device to add the number one and area code to *7654321 so that the device can forward a call to (1) (519) 765-4321, type remap0,*,1519,7,7. • To configure a device to forward 411 calls to your organization's help desk, type remap0,411,+15191231234,0,0. • To forward an international phone number to a toll free phone number, type remap0,+447700001111,18770001111,0,0.
Default value	• Null value

Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server 5.0 SP2

RIM Value-Added Applications policy group

Allow Edits to Application Server Proxy URLs for Microsoft SharePoint IT policy rule

Description	This rule specifies whether a BlackBerry device user can change the BlackBerry Social Networking Application Proxy URL and BlackBerry Social Networking Application Proxy File Service URL that the BlackBerry Client for Microsoft SharePoint uses.
Related rules	The Application Server Proxy URL for Microsoft SharePoint IT policy rule affects this rule. This rule requires that URLs are set in the Application Server Proxy URL for Microsoft SharePoint IT policy rule. The Application Server Proxy File Service URL for Microsoft SharePoint IT policy rule affects this rule. This rule requires that URLs are set in the Application Server Proxy File Server URL for Microsoft SharePoint IT policy rule.
Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server 5.0 SP3

Allow Edits to Microsoft SharePoint Site URLs IT policy rule

Description	This rule specifies whether a BlackBerry device user can access, add, change, or delete Microsoft SharePoint website URLs that are not listed in the Initial Microsoft SharePoint Site URL IT policy rule using a BlackBerry device.
Related rules	The Initial Microsoft SharePoint Site URL IT policy rule affects this rule. You specify the initial Microsoft SharePoint site URL in the Initial Microsoft SharePoint Site URL IT policy rule.
Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server 5.0 SP3

Allow Edits to BlackBerry Social Networking Application Proxy URL for Connections IT policy rule

Description	This rule specifies whether a BlackBerry device user can change the web address for the BlackBerry Social Networking Application Proxy on a BlackBerry device.
Related rules	The Lotus Connections IT policy rule affects this rule. You can use this rule when you configure the BlackBerry Social Networking Application Proxy URL for Lotus Connections IT policy rule.
Possible values	• Yes • No
Default value	• Yes

Rule introduction	• BlackBerry Enterprise Server 5.0 SP2

Allow Edits to BlackBerry Social Network Application Proxy URL for LotusQuickr IT policy rule

Description	This rule specifies whether a BlackBerry device user can change the URL for the BlackBerry Social Networking Application Proxy for IBMLotusQuickr on a BlackBerry device.
Related rules	The BlackBerry Social Networking Application Proxy Proxy URL for LotusQuickr IT policy rule affects this rule. You specify the URL for the BlackBerry Social Networking Application Proxy for LotusQuickr in the BlackBerry Social Networking Application Proxy Proxy URL for LotusQuickr IT policy rule.
Possible values	• Yes • No
Default value	• Yes
Rule introduction	• BlackBerry Enterprise Server 4.1 SP7

Allow TiVo for BlackBerry application IT policy rule

Description	This rule specifies whether TiVo for BlackBerry smartphones on the BlackBerry device is turned on.
Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry Device Software 4.2
Rule introduction	• BlackBerry Enterprise Server 4.1 SP7

Application Server Proxy File Service URL for Microsoft SharePoint IT policy rule

Description	This rule specifies the BlackBerry Social Networking Application Proxy File Service URL that the BlackBerry Client for Microsoft SharePoint uses. If you specify a value for this rule (for example, https://example.com:22445/fileservices-100), the BlackBerry Client for Microsoft SharePoint uses the URL that you specify.
Related rules	The Allow Edits to Application Server Proxy URLs for Microsoft SharePoint IT policy rule affects this rule. You can use the Allow Edits to Application Server Proxy URLs for Microsoft SharePoint IT policy rule to control whether the BlackBerry device user can change the URL.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server 5.0 SP3

Application Server Proxy URL for Microsoft SharePoint IT policy rule

Description	This rule specifies the BlackBerry Social Networking Application Proxy URL that the BlackBerry Client for Microsoft SharePoint uses. If you specify a value for this rule (for example, https://example.com:22443/sp-100/DeviceConnector), the BlackBerry Client for Microsoft SharePoint uses the URL when it starts for the first time.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server 5.0 SP3

BlackBerry Social Networking Application Proxy URL for Connections IT policy rule

Description	This rule specifies the web address for the server that hosts the BlackBerry Social Networking Application Proxy that the BlackBerry Client for IBM Connections can use. For example, https://<*server_name*>:<*port*>/lcs-230.
Related rules	This rule affects the Allow Edits to BlackBerry Social Networking Application Proxy URL for Lotus Connections IT policy rule. You must configure this rule before you can use the Allow Edits to BlackBerry Social Networking Application Proxy URL for Lotus Connections IT policy rule.
Default value	• Null value
Rule introduction	• BlackBerry Enterprise Server 5.0 SP2

BlackBerry Social Network Application Proxy URL for LotusQuickr IT policy rule

Description	This rule specifies the URL of the server that hosts the BlackBerry Social Networking Application Proxy that the BlackBerry Client for IBMLotusQuickr uses (for example, https://<*server_name*>:<*port*>/qkr-100/services/). If you do not configure this rule, a BlackBerry device user can access the host server by typing the URL on the BlackBerry device.
Related rules	This rule affects the Allow Edits to BlackBerry Social Network Application Proxy URL for LotusQuickr IT policy rule. If you configure this rule, you can use the Allow Edits to BlackBerry Social Network Application Proxy URL for LotusQuickr IT policy rule to control whether the user can change the URL of the host server.
Default value	• Null value
Rule introduction	• BlackBerry Enterprise Server 4.1 SP7

Deactivate eBay for BlackBerry smartphones IT policy rule

Description	This rule specifies whether a BlackBerry device can run the eBay app for BlackBerry smartphones.
Possible values	• Yes • No
Default value	• No
Rule introduction	• BlackBerry Enterprise Server 5.0 SP2

Disable Amazon MP3 for BlackBerry smartphones IT policy rule

Description	This rule specifies whether a BlackBerry device can run the Amazon MP3 for BlackBerry smartphones application.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server 5.0 SP3

Disable BlackBerry Radio

Description	This rule specifies whether a BlackBerry device can run the BlackBerry Radio application. If you set this rule to Yes, a user cannot use the he BlackBerry Radio application.
Possible values	• Yes • No
Default value	• No
Rule introduction	• BlackBerry Enterprise Server 5.0 SP4

Disable BlackBerry Wallet IT policy rule

Description	This rule specifies whether to prevent BlackBerry Wallet from running on a BlackBerry device.
Possible values	• Yes • No
Default value	• No
Rule introduction	• BlackBerry Enterprise Server 4.1 SP6

Disable Ecommerce Content Optimization Engine IT policy rule

Description	This rule specifies whether to prevent the ecommerce content optimization engine for the BlackBerry Browser from running on a BlackBerry device.
Possible values	• Yes • No

Default value	• No
Rule introduction	• BlackBerry Enterprise Server 4.1 SP6

Disable Feeds application IT policy rule

Description	This rule specifies whether a BlackBerry device can run the Feeds application. The Feeds application permits a BlackBerry device user to monitor activity in a social-networking account and display the latest news and information in a web feed.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry 6
Rule introduction	• BlackBerry Enterprise Server 5.0 SP2

Disable Lotus Connections IT policy rule

Description	This rule specifies whether to prevent IBM Connections from running on a BlackBerry device.
Possible values	• Yes • No
Default value	• No
Rule introduction	• BlackBerry Enterprise Server 4.1 SP6

Disable Geo-Location in Social Networking Applications IT policy rule

Description	This rule specifies whether social-networking applications on a BlackBerry device can associate or share geo-location information with social-networking services (for example, Twitter orFacebook).
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Enterprise Server 4.1 SP5
Rule introduction	• BlackBerry Enterprise Server 5.0 SP3

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.
Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry Device Software 4.2.0
Rule introduction	• BlackBerry Enterprise Server 4.1.7

Disable RIM Value-Added Applications IT policy rule

Description	This rule specifies whether to prevent value-added applications that Research In Motion developed from running on a BlackBerry device. This rule does not apply to BlackBerry Maps, some instant-messaging applications, some public photo-sharing applications, Facebook, BlackBerry MDS Runtime Applications, and device diagnostic applications. For more information about the applications, see the application-specific IT policy rules.
Possible values	• False • No
Default value	• No
Rule introduction	• BlackBerry Enterprise Server 4.1 SP6

Enable the "Tell A Friend" Feature in BlackBerry Client for Connections IT policy rule

Description	This rule specifies whether a BlackBerry device user can use the Tell a Friend feature in the BlackBerry Client for IBM Connections to recommend the BlackBerry Client for IBM Connections to another user.
Possible values	• Yes • No
Default value	• Yes
Rule introduction	• BlackBerry Enterprise Server 5.0 SP2

Enable the "Tell A Friend" Feature in BlackBerry Client for LotusQuickr IT policy rule

Description	This rule specifies whether the Tell a Friend feature is turned on in the BlackBerry Client for IBMLotusQuickr.
Possible values	• Yes • No
Default value	• Yes
Rule introduction	• BlackBerry Enterprise Server 4.1 SP7

Enable the "Tell A Friend" Feature in BlackBerry Client for Microsoft SharePoint IT policy rule

Description	This rule specifies whether the Tell a Friend feature is turned on for the BlackBerry Client for Microsoft SharePoint. The Tell a Friend Feature lets a BlackBerry device user send an email invitation that contains a link that the recipient can use to download the BlackBerry Client for Microsoft SharePoint.
Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server 5.0 SP3

Initial Microsoft SharePoint Site Name IT policy rule

Description	This rule specifies the display name for the Microsoft SharePoint website that is specified in the Initial Microsoft SharePoint Site URL IT policy rule. If you set a value for this rule, the BlackBerry Client for Microsoft SharePoint displays this name.
Related rules	The Initial Microsoft SharePoint Site URL IT policy rule affects this rule. You specify the URL that this name describes in the Initial Microsoft SharePoint Site URL IT policy rule.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server 5.0 SP3

Initial Microsoft SharePoint Site URL IT policy rule

Description	This rule specifies the URL of the Microsoft SharePoint website that the BlackBerry Client for Microsoft SharePoint browses to when it starts for the first time. If you do not specify a URL in this rule and do not set the Allow Edits to Microsoft SharePoint Site URLs IT policy rule to Yes, a BlackBerry device user cannot start the BlackBerry Client for Microsoft SharePoint. If you change this rule after the user starts the BlackBerry Client for Microsoft SharePoint for the first time, the BlackBerry Client for Microsoft SharePoint does not browse to the website that you specify when it starts.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server 5.0 SP3

Connections Activities Server IT policy rule

Description	This rule specifies the address of the server that hosts the IBM Connections Activities component. If you configure this rule, a BlackBerry device user can use the specified server address only. If you do not configure this rule, the user must specify the server address manually.
Default value	• Null value
Minimum requirements	• BlackBerry Client for IBM Connections 1.0
Rule introduction	• BlackBerry Enterprise Server 4.1 SP6

Lotus Connections Blogs Server IT policy rule

Description	This rule specifies the address of the server that hosts the IBM Connections Blogs component. If you configure this rule, a BlackBerry device user can use the specified server address only. If you do not configure this rule, the user must specify the server address manually.
Default value	• Null value
Minimum requirements	• BlackBerry Client for IBM Connections 1.0
Rule introduction	• BlackBerry Enterprise Server 4.1 SP6

Lotus Connections Communities Server IT policy rule

Description	This rule specifies the address of the server that hosts the IBM Connections Communities component. If you configure this rule, a BlackBerry device user can use the specified server address only. If you do not configure this rule, the user must specify the server address manually.
Default value	• Null value

Minimum requirements	• BlackBerry Client for IBM Connections 1.0
Rule introduction	• BlackBerry Enterprise Server 4.1 SP6

Lotus Connections Dogear Server IT policy rule

Description	This rule specifies the address of the server that hosts the IBM Connections Dogear component. If you configure this rule, a BlackBerry device user can use the specified server address only. If you do not configure this rule, the user must specify the server address manually.
Default value	• Null value
Minimum requirements	• BlackBerry Client for IBM Connections 1.0
Rule introduction	• BlackBerry Enterprise Server 4.1 SP6

Connections Profiles Server IT policy rule

Description	This rule specifies the address of the server that hosts the IBM Connections Profiles component. If you configure this rule, a BlackBerry device user can use the specified server address only. If you do not configure this rule, the user must specify the server address manually.
Default value	• Null value
Minimum requirements	• BlackBerry Client for IBM Connections 1.0
Rule introduction	• BlackBerry Enterprise Server 4.1 SP6

Plans Application IT policy rule

Description	This rule specifies whether a BlackBerry device can run the Plans application. If you set this rule to Disallow, users cannot use the Plans application.
Possible values	• Allow • Disallow
Default value	• Allow
Minimum requirements	• BlackBerry Device Software 4.5
Rule introduction	• BlackBerry Enterprise Server 5.0 SP4 • KB31693

Prevent BlackBerry Mobile Media Sync over a Wi-Fi network IT policy rule

Description	This rule specifies whether a BlackBerry device user can use BlackBerryWi-Fi music sync to synchronize media files over a Wi-Fi network.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry 6
Rule introduction	• BlackBerry Enterprise Server 5.0 SP3

Prevent BlackBerry Podcasts IT policy rule

Description	This rule specifies whether a BlackBerry device user can run BlackBerry Podcasts on a BlackBerry device. BlackBerry Podcasts permits a user to view, manage, and play any audio podcasts or video podcasts that are stored on the device or in an external memory file system.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry 6 • BlackBerry Desktop Software 6.0
Rule introduction	• BlackBerry Enterprise Server 5.0 SP2

Prevent RSS Feeds IT policy rule

Description	This rule specifies whether a BlackBerry device user can use the Feeds application on a BlackBerry device to subscribe to RSS feeds.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry 6
Rule introduction	• BlackBerry Enterprise Server 5.0 SP2

Prevent uploading of videos to YouTube IT policy rule

Description	This rule specifies whether a BlackBerry device user can upload videos to YouTube using the YouTube video uploader for BlackBerry smartphones.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry 6 • BlackBerry Desktop Software 6.0
Rule introduction	• BlackBerry Enterprise Server 5.0 SP2

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.
Default value	• Null value
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise

Minimum requirements	• BlackBerry Device Software 4.0 • S/MIME Support Package for BlackBerry smartphones 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0 SP3

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.
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
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise
Minimum requirements	• BlackBerry Device Software 3.6 • S/MIME Support Package for BlackBerry smartphones 1.5
Rule introduction	• BlackBerry Enterprise Server 4.0 SP3

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.
Possible values	• Automatic • Manual • None
Default value	• Automatic
Minimum requirements	• BlackBerry Device Software 4.5
Rule introduction	• BlackBerry Enterprise Server 4.1 SP5

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.
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 4.1 SP6

S/MIME Attachment Support IT policy rule

Description	This rule specifies how a BlackBerry device processes S/MIME-protected messages that include attachments.
Possible values	• None • End-to-End • End-to-End or Trusted BES
Default value	• End-to-End or Trusted BES
Minimum requirements	• BlackBerry 7
Rule introduction	• BlackBerry Enterprise Server 5.0 SP3

S/MIME Blind Copy Address IT policy rule

Description	This rule specifies an email address that is added as a BCC recipient to S/MIME-protected email messages that a BlackBerry device user sends.
Default value	• Null value
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise
Minimum requirements	• BlackBerry Device Software 3.6 • S/MIME Support Package for BlackBerry smartphones 1.5
Rule introduction	• BlackBerry Enterprise Server 4.0 SP3

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.
Possible values	• Yes • No
Default value	• No
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise
Minimum requirements	• BlackBerry Device Software 3.6 • S/MIME Support Package for BlackBerry smartphones 1.5
Rule introduction	• BlackBerry Enterprise Server 4.0 SP3

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.
Possible values	• Yes • No
Default value	• No
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise
Minimum requirements	• BlackBerry Device Software 3.6 • S/MIME Support Package for BlackBerry smartphones 1.5

Rule introduction	• BlackBerry Enterprise Server 4.0 SP3

S/MIME Force Smartcard Use IT policy rule

Description	This rule specifies whether a BlackBerry device must perform all operations that use certificates while the device is attached to a BlackBerry Smart Card Reader.
Possible values	• Yes • No
Default value	• No
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise
Minimum requirements	• BlackBerry Device Software 3.6 • S/MIME Support Package for BlackBerry smartphones 1.5
Rule introduction	• BlackBerry Enterprise Server 4.0 SP3

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.
Possible values	• 512 to 4096 bits
Default value	• 1024 bits
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise
Minimum requirements	• BlackBerry Device Software 3.6 • S/MIME Support Package for BlackBerry smartphones 1.5

Rule introduction	• BlackBerry Enterprise Server 4.0 SP3

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.
Possible values	• 512 to 1024 bits
Default value	• 1024 bits
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise
Minimum requirements	• BlackBerry Device Software 3.6 • S/MIME Support Package for BlackBerry smartphones 1.5
Rule introduction	• BlackBerry Enterprise Server 4.0 SP3

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.
Possible values	• 163 to 571 bits
Default value	• 163 bits
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise
Minimum requirements	• BlackBerry Device Software 3.6 • S/MIME Support Package for BlackBerry smartphones 1.5

Rule introduction	• BlackBerry Enterprise Server 4.0 SP3

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.
Possible values	• 512 to 4096 bits
Default value	• 1024 bits
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise
Minimum requirements	• BlackBerry Device Software 3.6 • S/MIME Support Package for BlackBerry smartphones 1.5
Rule introduction	• BlackBerry Enterprise Server 4.0 SP3

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.
Possible values	• Automatic • Manual • None
Default value	• Manual
Minimum requirements	• BlackBerry Device Software 5.0

Rule introduction	• BlackBerry Enterprise Server 5.0 SP1

SIM Application Toolkit policy group

Disable Bearer Independent Protocol IT policy rule

Description	This rule specifies whether the SIM card in a BlackBerry device can open a data connection using BIP. BIP is a protocol that allows communication between wireless service providers and SIM cards.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry 6
Rule introduction	• BlackBerry Enterprise Server 5.0 SP3

Disable Network Location Query IT policy rule

Description	This rule specifies whether to prevent a wireless network or SIM card from querying a BlackBerry device for location-related information. The information that the SIM card can query is limited to the current wireless network and cell identities, device IMEI, date, time, and some measurement results.
Possible values	• Yes • No
Default setting	• No
Minimum requirements	• BlackBerry Device Software 3.6

Rule introduction	• BlackBerry Enterprise Server 4.0 SP3

Disable SIM Call Control IT policy rule

Description	This rule specifies whether to prevent a SIM card from changing a call, a supplementary service request, or an SMS text message.
Possible values	• Yes • No
Default setting	• No
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server 4.0 SP3

Disable SIM Originated Calls IT policy rule

Description	This rule specifies whether to prevent a SIM card from making a call, performing a supplementary service operation, or sending an SMS text message.
Possible values	• Yes • No
Default setting	• No
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server 4.0 SP3

Secure Email policy group

The IT policy rules in the Secure Email 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*.

Canonical Certificate Domain Name IT policy rule

Description	This rule specifies the domain name for the email addresses that are contained in certificates that are issued within your organization. This rule is intended for use in organizations where BlackBerry device users' certificates contain a long-lived email address, but users typically send email messages from a shorter-lived email address with the same username component and a different domain component. Specify the domain name that is used for the email addresses that are contained in certificates that are issued within the organization. Use a comma (,) to separate multiple domain names.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.2
Rule introduction	• BlackBerry Enterprise Server 4.0 SP6

Disable Certificate Address Checks IT policy rule

Description	This rule specifies whether a warning appears if a BlackBerry device user receives a signed email message and the sender's email address does not appear in the certificate or PGP key that was used to sign the email message.
Possible values	• Yes • No
Default value	• No

Minimum requirements	• BlackBerry Device Software 4.2
Rule introduction	• BlackBerry Enterprise Server 4.0 SP6

Suggest Default Encoding for All Outgoing Email and PIN Messages IT policy rule

Description	This rule specifies whether a BlackBerry device suggests the default encoding or the encoding based on the message history for outgoing email and PIN messages. If you set this rule to Allowed, a BlackBerry device user can select whether to use the default encoding or the encoding based on the message history. If you set this rule to Required, the device suggests the default encoding. If you set this rule to Disallowed, the device suggests the encoding based on the message history.
Possible values	• Allowed • Required • Disallowed
Default value	• Allowed
Minimum requirements	• BlackBerry 7
Rule introduction	• BlackBerry Enterprise Server 5.0 SP4 • KB28284

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
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise only with devices that are running BlackBerry Device Software 4.0 or later
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server for Microsoft Exchange 3.6 • BlackBerry Enterprise Server for IBM Domino 4.0 • BlackBerry Enterprise Server for Novell GroupWise 4.0

Allow Internal Connections IT policy rule

Description	This rule specifies whether applications, including third-party applications, can initiate internal connections (for example, to websites behind your organization's firewall using the BlackBerry MDS Connection Service).
Possible values	• Yes • No

Default value	• Yes
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise only with devices that are running BlackBerry Device Software 4.0 or later
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server for Microsoft Exchange 3.6 • BlackBerry Enterprise Server for IBM Domino 4.0 • BlackBerry Enterprise Server for Novell GroupWise 4.0

Allow Outgoing Call When Locked IT policy rule

Description	This rule specifies whether a BlackBerry device user can make calls from a locked BlackBerry device.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0

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 4.1 SP4

Allow Screen Shot Capture IT policy rule

Description	This rule specifies whether a BlackBerry device permits applications, including third-party applications, to take screen shots.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.2.2
Rule introduction	• BlackBerry Enterprise Server 4.1 SP4

Allow Smart Card Password Caching IT policy rule

Description	This rule specifies whether a BlackBerry device can cache the smart card password.
Related rules	This rule affects the Key Store Password Maximum Timeout IT policy rule. If you configure this rule, you should also configure the Key Store Password Maximum Timeout IT policy rule.
Possible values	• Yes • No

Default value	• No
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0

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
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise only with devices that are running BlackBerry Device Software 4.0 or later
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server for Microsoft Exchange 3.6 • BlackBerry Enterprise Server for IBM Domino 4.0 • BlackBerry Enterprise Server for Novell GroupWise 4.0

Allow Synchronization of Data From Voice Enabled Search IT policy rule

Description	This rule specifies whether a BlackBerry device can synchronize voice search data for address book names with a server. If you set this rule to Yes, the device can synchronize the voice search data with a server. Synchronizing data can improve the accuracy of voice searches.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry 7
Rule introduction	• BlackBerry Enterprise Server 5.0 SP4 • KB28284

Allow Third Party Apps to Access Screen Contents IT policy rule

Description	This rule specifies whether a third-party application on a BlackBerry device can access the data that is displayed on the device screen.
Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server 5.0 SP3

Allow Third Party Apps to Use Persistent Store IT policy rule

Description	This rule specifies whether third-party applications can use the persistent store API on a BlackBerry device. In later versions of the BlackBerry Enterprise Server, use the Is access to the interprocess communication API allowed application control policy rule to specify whether applications can access the persistent store API. This rule is obsolete in BlackBerry Enterprise Server 3.6 SP2.
Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server 3.6

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.
Possible values	• Yes • No
Default value	• Yes
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise only on devices that are running BlackBerry Device Software 4.0 or later
Minimum requirements	• BlackBerry Device Software 3.6

Rule introduction	• BlackBerry Enterprise Server for Microsoft Exchange 3.6 • BlackBerry Enterprise Server for IBM Domino 4.0 • BlackBerry Enterprise Server for Novell GroupWise 4.0

Allow Voice Enabled Search IT policy rule

Description	Specifies whether a BlackBerry device user can use voice enabled search on a device. If you set this rule to Yes, the user can use voice commands to interact with the search feature on the device.
Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry 7
Rule introduction	• BlackBerry Enterprise Server 5.0 SP4 • KB28284

Allowed Authentication Mechanisms IT policy rule

Description	This rule specifies the types of authentication mechanisms that a BlackBerry device user can turn on. Authentication mechanisms control the user's access to a BlackBerry device.
Related rules	This rule affects the Force Smart Card Two Factor Authentication IT policy rule. This rule takes priority over the Force Smart Card Two Factor Authentication IT policy rule. For example, if you configure this rule to prevent smart card authentication but the Force Smart Card Two Factor Authentication IT policy rule is configured to Yes, smart card authentication is not forced.
Possible values	• Smartcard • Fingerprint • Smartcard and Fingerprint • Proximity

	• Other
Default value	• Smartcard, Fingerprint, Smartcard and Fingerprint, Proximity, and Other
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server 5.0

Application Installation from Specific URLs Only IT policy rule

Description	This rule specify a list of web addresses that a BlackBerry device user can download applications from. You must separate multiple web addresses with a comma (,). Each address must be a fully qualified domain name or a wildcard domain name that starts with a period (.). If you specify a web address in this rule, the browser uses the BlackBerry MDS Connection Service to connect to the web address, even if the web address is not listed in the MDS Browser Domains IT policy rule.
Related rule	This rule is affected by the Application Installation Methods IT policy rule. If the Application Installation Methods rule is set to Disallow Browser, the device ignores this rule.
Default value	• Null value
Minimum requirements	• BlackBerry 7.1
Rule introduction	• BlackBerry Enterprise Server 5.0 SP4 • KB29510

Application Installation Methods IT policy rule

Description	This rule specifies application installation methods that a BlackBerry device user cannot use to install applications on the device. You can prevent a user from using the BlackBerry App World storefront, the device browser, a media card, and a USB connection.

Related rules	This rule affects the Disallow Third Party Application Downloads IT policy rule. If you set this rule it takes precedence over the Disallow Third Party Application Downloads rule on BlackBerry 7.1 and higher devices.
Possible values	• Disallow App World • Disallow Browser • Disallow Media Card • Disallow USB
Default value	• Null value
Minimum requirements	• BlackBerry 7.1
Rule introduction	• BlackBerry Enterprise Server 5.0 SP4 • KB29510

Certificate Status Cache Timeout IT policy rule

Description	This rule specifies the maximum number of days that a BlackBerry device saves the certificate status. This rule does not apply to any devices. This rule is obsolete in BlackBerry Enterprise Server 5.0.
Possible values	• 1 to 365 days
Default value	• 7 days
Rule introduction	• BlackBerry Enterprise Server 4.0

Certificate Status Maximum Expiry Time IT policy rule

Description	This rule specifies the maximum amount of time that a certificate status can remain on a BlackBerry device before it should be updated in the key store on the device and in the certificate synchronization tool of the BlackBerry Desktop Manager.
Possible values	• 1 to 4380 hours
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0

Content Protection of Contact List IT policy rule

Description	This rule specifies whether the contact list on a BlackBerry device is included in content protection when content protection is turned on. If you set this rule to Allowed, the BlackBerry device user can choose to include the contact list in content protection. If you set this rule to Required, the contact list is include in content protection. If you set this rule to Disallowed, the contact list is not included in content protection and the user cannot choose to include the contact list in content protection. If the contact list is content-protected and the device is locked, the device does not permit call display and does not share contacts over a Bluetooth connection. Devices that are running BlackBerry Device Software 4.7 and earlier process the Disallowed setting in the same way that as the Required setting. The previous name of this rule was Force Include Address Book In Content Protection.
Possible values	• Allowed • Required • Disallowed
Default value	• Allowed

Minimum requirements	• BlackBerry Device Software 4.2
Rule introduction	• BlackBerry Enterprise Server 4.0 SP6

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	• Strong in the Advanced security IT policy and Advanced security with No 3rd Applications IT policy • Null value in all other preconfigured IT policies
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0

Content Protection Usage IT policy rule

Description	This rule specifies whether content protection is available on a BlackBerry device. If you set this rule to Allowed, a BlackBerry device user can turn on content protection on the device. This rule does not turn on content protection. To turn on content protection, you must configure the Content Protection Strength IT policy rule or the user must configure content protection on the device in the device options. For more information about content protection, see the *BlackBerry Enterprise Solution Security Technical Overview*.
Possible values	• Allowed • Disallowed
Default value	• Allowed
Minimum requirements	• BlackBerry 6
Rule introduction	• BlackBerry Enterprise Server 5.0 SP2

Desktop Backup IT policy rule

Description	This rule specifies which BlackBerry device databases are backed up by the BlackBerry Desktop Software.
Possible values	• All databases • Minimal subset of databases • No databases • No organizational databases
Default value	• All databases
Minimum requirements	• BlackBerry Device Software 4.0

Rule introduction	• BlackBerry Enterprise Server 4.0

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 4.0

Disable BlackBerry App World IT policy rule

Description	This rule specifies whether the BlackBerry App World storefront on a BlackBerry device is turned off. This rule is obsolete in BlackBerry Enterprise Server 5.0 SP2 and later and BlackBerry App World 2.0 and later. In BlackBerry Enterprise Server 5.0 SP2 and later and BlackBerry App World 2.0 and later, configure the Disable App World IT policy rule in the BlackBerry App World policy group.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.2
Rule introduction	• BlackBerry Enterprise Server 4.1 SP7

Disable Browsing Of Remote Shared Folders IT policy rule

Description	This rule specifies whether a BlackBerry device user can browse shared folders and files located on the servers in your organization's network using the file browser on a BlackBerry device.
Possible values	• Yes • No
Default values	• No
Minimum requirements	• BlackBerry 6
Rule introduction	• BlackBerry Enterprise Server 5.0 SP2

Disable Certificate or Key Import From External Memory IT policy rule

Description	This rule specifies whether a BlackBerry device can import certificates and PGP keys, including private keys, from a media card.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server 5.0 SP1

Disable Cut/Copy/Paste IT policy rule

Description	This rule specifies whether to prevent a BlackBerry device user from cutting, copying, and pasting text on a BlackBerry device.
Possible value	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0

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 4.0 SP6

Disable Forwarding Between Services IT policy rule

Description	This rule specifies whether a BlackBerry device user can reply to or forward an email message using an email account or messaging service (for example, the BlackBerry Enterprise Server or BlackBerry Internet Service) that is different from the email account or messaging service that user received the email message with.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0

Disable Geo-Tagging of Photos IT policy rule

Description	This rule specifies whether to prevent a BlackBerry device from adding geographical co-ordinates to the metadata of stored pictures.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.2
Rule introduction	• BlackBerry Enterprise Server 4.1 SP4

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 4.1 SP5

Disable Invalid Certificate Use IT policy rule

Description	This rule specifies whether to prevent a BlackBerry device user from sending an email message from a BlackBerry device using an expired or invalid certificate.
Possible value	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 3.6 • BlackBerry Enterprise Server for IBM Domino 4.0 • BlackBerry Enterprise Server for Novell GroupWise 4.0
Rule introduction	• BlackBerry Enterprise Server 3.6

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 4.0

Disable Key Store Backup IT policy rule

Description	This rule specifies whether to prevent a BlackBerry device user from backing up the certificates and private keys that are stored on a BlackBerry device.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0

Disable Key Store Low Security IT policy rule

Description	This rule specifies whether to prevent a BlackBerry device user from setting the key store security level to Low. For BlackBerry devices that are running BlackBerry Device Software 3.6, the next highest

	security level is High. For devices that are running BlackBerry Device Software 4.0 or later, the next highest security level is Medium.
Possible values	• Yes • No
Default value	• No
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise only with devices that are running BlackBerry Device Software 4.0 or later
Minimum requirements	• BlackBerry Device Software 3.6 • BlackBerry Enterprise Server for IBM Domino 4.0 • BlackBerry Enterprise Server for Novell GroupWise 4.0
Rule introduction	• BlackBerry Enterprise Server 3.6

Disable Media Manager FTP Access IT policy rule

Description	This rule specifies whether applications can access the FTP channel from the media manager tool in the BlackBerry Desktop Manager. This rule controls whether a BlackBerry device can transfer files from the onboard device memory or media card using the FTP channel. When you permit the device to transfer files using FTP, the device does not protect the files using content protection. The device can encrypt the data on the media card 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.
Possible values	• Yes • No
Default value	• No
Exceptions	• BlackBerry Desktop Manager 4.2.2 • BlackBerry Enterprise Server for Novell GroupWise

Minimum requirements	• BlackBerry Device Software 4.2
Rule introduction	• BlackBerry Enterprise Server 4.0 SP6

Disable Message Normal Send IT policy rule

Description	This rule specifies whether to require a BlackBerry device user to send encrypted or signed email messages. For BlackBerry devices that are running BlackBerry Device Software 5.0 and later, this rule applies only to email messages that a user sends through your organization's BlackBerry Enterprise Server. To prevent a user from sending email messages that are not encrypted or signed from a different messaging service such as the BlackBerry Internet Service, configure the Allow Other Message Services rule in the Service Exclusivity policy group. For BlackBerry devices that are running BlackBerry Device Software 4.7 and earlier, this rule applies to all messaging services.
Possible values	• Yes • No
Default value	• No
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise only with devices that are running BlackBerry Device Software 4.0 or later
Minimum requirements	• BlackBerry Device Software 3.6 • BlackBerry Enterprise Server for IBM Domino 4.0 • BlackBerry Enterprise Server for Novell GroupWise 4.0
Rule introduction	• BlackBerry Enterprise Server 3.6

Disable Peer-to-Peer Normal Send IT policy rule

Description	This rule specifies whether to prevent a BlackBerry device user from sending PIN messages that are not encrypted when using the S/MIME Support Package for BlackBerry smartphones or PGP Support Package for BlackBerry smartphones.
Possible values	• Yes • No
Default value	• No
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise only with devices that are running BlackBerry Device Software 4.0 or later
Minimum requirements	• BlackBerry Device Software 3.6 • BlackBerry Enterprise Server for IBM Domino 4.0 • BlackBerry Enterprise Server for Novell GroupWise 4.0
Rule introduction	• BlackBerry Enterprise Server 3.6

Disable Persisted Plain Text IT policy rule

Description	This rule specifies whether to prevent applications from keeping the plain-text form of a content-protected object in the persistent store on a BlackBerry device. Configure this rule only if you require that sensitive data does not persist in plain-text form on a device. **Attention:** If you change this rule to Yes, applications on the device that do not use the content protection framework API to encrypt data might not work.
Possible values	• Yes • No
Default value	• No

Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0

Disable Public Photo Sharing Applications IT policy rule

Description	This rule specifies whether to prevent a BlackBerry device user from uploading pictures to the Internet using public photo sharing applications.
Possible values	• Yes • No
Default value	• No
Rule introduction	• BlackBerry Enterprise Server 4.1 SP4

Disable Public Social Networking Applications IT policy rule

Description	This rule specifies whether a BlackBerry device user can install public social networking applications on a BlackBerry device to access public social networking services.
Possible values	• Yes • No
Default value	• No
Rule introduction	• BlackBerry Enterprise Server 4.1 SP5

Disable Radio When Cradled IT policy rule

Description	This rule specifies whether a BlackBerry device turns off the wireless transceiver when it connects to a USB device.
Possible values	• Radio disabled when USB device is connected • Radio not disabled when USB device is connected • Radio disabled when the connected USB device enumerates
Default value	• Radio not disabled when USB device is connected
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0

Disable Revoked Certificate Use IT policy rule

Description	This rule specifies whether to prevent a BlackBerry device user from sending email messages that are encrypted using revoked certificates.
Possible values	• Yes • No
Default value	• No
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise only with devices running BlackBerry Device Software 4.0 or later
Minimum requirements	• BlackBerry Device Software 3.6 • BlackBerry Enterprise Server for IBM Domino 4.0 • BlackBerry Enterprise Server for Novell GroupWise 4.0

Rule introduction	• BlackBerry Enterprise Server for Microsoft Exchange 3.6

Disable Smart Password Entry IT policy rule

Description	This rule specifies whether to prevent a BlackBerry device user from using smart password entry with two-factor authentication. Smart password entry allows the user to enter numeric passwords on the BlackBerry device without pressing the Alt key.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.2
Rule introduction	• BlackBerry Enterprise Server 4.0 SP6

Disable Stale Certificate Status Checks IT policy rule

Description	This rule specifies whether a BlackBerry device displays warnings and indicators if a user tries to use a certificate with a stale status.
Related rules	This rule affects the Certificate Status Maximum Expiry Time IT policy rule. If you set this rule to Yes, the device ignores the Certificate Status Maximum Expiry Time IT policy rule and the status of certificates on the device never expires.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.2

Rule introduction	• BlackBerry Enterprise Server 4.0 SP6

Disable Stale Status Use IT policy rule

Description	This rule specifies whether to prevent a BlackBerry device user from sending an email message that is encrypted using a certificate with a stale status.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0

Disable Untrusted Certificate Use IT policy rule

Description	This rule specifies whether to prevent a BlackBerry device user from sending an email message that is encrypted with a certificate that the BlackBerry device does not trust.
Possible values	• Yes • No
Default value	• No
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise only with devices that are running BlackBerry Device Software 4.0 or later
Minimum requirements	• BlackBerry Device Software 3.6 • BlackBerry Enterprise Server for IBM Domino 4.0 • BlackBerry Enterprise Server for Novell GroupWise 4.0

Rule introduction	• BlackBerry Enterprise Server 3.6

Disable Unverified Certificate Use IT policy rule

Description	This rule specifies whether to prevent a BlackBerry device user from sending an email message that is encrypted with a certificate that the BlackBerry device cannot verify.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0

Disable Unverified CRLs IT policy rule

Description	This rule specifies whether to prevent a BlackBerry device user from accepting CRLs that are not verified on the BlackBerry MDS Connection Service when checking the status of a certificate.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0

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 Advanced security IT policy and Advanced Security with No 3rd Party Applications IT policy • No in all other preconfigured IT policies
Minimum requirements	• BlackBerry Device Software 4.2
Rule introduction	• BlackBerry Enterprise Server 4.0 SP6

Disable Weak Certificate Use IT policy rule

Description	This rule specifies whether to prevent a BlackBerry device user from sending an email message using a certificate that has a corresponding weak public key. Use the IT policy rules that are provided for the TLS application, WTLS application, S/MIME Support Package for BlackBerry smartphones, or PGP Support Package for BlackBerry smartphones to configure the minimum strengths for the RSA, DSA, ECC, and Diffie-Hellman algorithm key lengths.
Possible values	• Yes • No

Default value	• No
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise only with devices that are running BlackBerry Device Software 4.0 or later
Minimum requirements	• BlackBerry Device Software 3.6 • BlackBerry Enterprise Server for IBM Domino 4.0 • BlackBerry Enterprise Server for Novell GroupWise 4.0
Rule introduction	• BlackBerry Enterprise Server 3.6

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	• Yes in the Medium password security with No 3rd Party Applications IT policy rule and the Advanced security with No 3rd Party Applications IT policy rule • No in all other preconfigured IT policies
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise only with devices that are running BlackBerry Device Software 4.0 or later
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server for Microsoft Exchange 3.6 • BlackBerry Enterprise Server for IBM Domino 4.0 • BlackBerry Enterprise Server for Novell GroupWise 4.0

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 5.0 SP1

Enforce FIPS Mode of Operation IT policy rule

Description	This rule specifies whether a BlackBerry device must operate in FIPS mode. FIPS are computer-system standards that were developed by the United States federal government. AES must be the transport algorithm for the device to operate in the FIPS mode of operation.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry 7
Rule introduction	• BlackBerry Enterprise Server 5.0 SP3

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	• Encrypt to User Password (excluding multimedia directories) in the Advanced Security IT policy and Advanced Security with No 3rd Party Applications IT policy • Not required in all other preconfigured IT policies
Minimum requirements	• BlackBerry Device Software 4.2
Rule introduction	• BlackBerry Enterprise Server 4.0 SP6

FIPS Level IT policy rule

Description	This rule specifies the level of FIPS compliance that your organization requires. If you change this rule to Level 2, a BlackBerry device prevents WTLS from using an RC encryption algorithm, which can cause problems when using WTLS. This rule is obsolete in BlackBerry Enterprise Server 4.1 SP3 and later and BlackBerry Device Software 4.2.1 and later.
Related rules	This rule affects the Password Required IT policy rule. If you change this rule to Level 2, the Password Required IT policy rule is configured to Yes. This rule affects the Minimum Password Length IT policy rule. If you change this rule to Level 2, the Minimum Password Length IT policy rule is configured to 5. This rule affects the Suppress Password Echo IT policy rule. If you change this rule to Level 2, the Suppress Password Echo IT policy rule is configured to Yes. This rule affects the PGP Allowed Content Ciphers IT policy rule. If you change this rule to Level 2, the PGP Allowed Content Ciphers IT policy rule is configured to AES (256-bit), AES (192-bit), AES (128-bit), Triple DES. This rule affects the S/MIME Allowed Content Ciphers IT policy rule. If you change this rule to Level 2, the S/MIME Allowed Content Ciphers IT policy rule is configured to AES (256-bit), AES (192-bit), AES (128-bit), Triple DES. This rule affects the TLS Restrict FIPS Ciphers IT policy rule. If you change this rule to Level 2, the TLS Restrict FIPS Ciphers IT policy rule is configured to Yes. This rule affects the Disallow Third Party Application Download IT policy rule. If you change this rule to Level 2, the Disallow Third Party Application Download IT policy rule is configured to Yes.
Possible values	• FIPS 140-2 Level 1 compliance • FIPS 140-2 Level 2 compliance

Default value	• FIPS 140-2 Level 1 compliance
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise only with devices that are running BlackBerry Device Software 4.0 to 4.2.1
Minimum requirements	• For FIPS Level 1 compliance, BlackBerry Device Software 3.3 • For FIPS Level 2 compliance, BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0

Firewall Block Incoming Messages IT policy rule

Description	This rule specifies whether the BlackBerry device firewall prevents the device from processing specific types of incoming messages. If you configure this rule, the device blocks the incoming messages that you specify at the firewall and does not notify a BlackBerry device user that those messages were received. The user can specify whether to block public PIN messages on a device. A user cannot specify whether to block organization-specific PIN messages on a device.
Possible values	• SMS messages • MMS messages • BlackBerry Internet Service messages • PIN messages (Public) • PIN messages (Corporate) • Enterprise messages
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.2
Rule introduction	• BlackBerry Enterprise Server 4.0 SP6

Firewall Whitelist Addresses IT policy rule

Description	This rule specifies whether **Content Protection of Contact List** is available.
Related rules	This rule affects the Content Protection of Contact List IT policy rule. If you configure this rule, the **Include contact list** option under **Security** > **Encryption** on the BlackBerry device is unchecked and locked.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.5
Rule introduction	• BlackBerry Enterprise Server 4.1 SP5

Force Content Protection Of Master Keys IT policy rule

Description	This rule specifies whether content protection for device transport keys that a BlackBerry device stores is turned on. Content protection is designed to encrypt the device transport keys on a device using 256-bit AES and store them in the device memory. To turn on content protection for device transport keys, you or a BlackBerry device user must turn on content protection on the device. You can turn on content protection on the device using the Content Protection Strength IT Policy Rule.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.1
Rule introduction	• BlackBerry Enterprise Server 4.0 SP3

Force Cryptographic Power Analysis Protection IT policy rule

Description	This rule specifies whether a BlackBerry device must use algorithms that are protected by cryptographic power analysis, if the algorithms are available.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry 7
Rule introduction	• BlackBerry Enterprise Server 5.0 SP4 • KB28284

Force Device Password Entry While User Authentication is Enabled IT policy rule

Description	This rule specifies whether a BlackBerry device user must type the BlackBerry device password in addition to the user-authentication credentials for the second-factor authentication method to unlock the device.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server 5.0 SP2

Force Display IT Policy Viewer Icon on Homescreen IT policy rule

Description	This rule specifies whether a BlackBerry device displays the IT Policy Viewer icon in the Application folder on the device. The IT policy viewer permits a BlackBerry device user to view IT policy rules from the Security policy group and Password policy group that have values that you configured for the device. Only devices that you activate on a BlackBerry Enterprise Server include the IT policy viewer.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry 6
Rule introduction	• BlackBerry Enterprise Server 5.0 SP2

Force LED Blinking When Microphone Is On IT policy rule

Description	This rule specifies whether a BlackBerry device LED flashes while the microphone is on (for example, during a call or when recording a voice message).
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.1
Rule introduction	• BlackBerry Enterprise Server 4.0 SP3

Force Lock When Closed IT policy rule

Description	This rule specifies whether BlackBerry Pearl Flip Series smartphones are security locked automatically when a BlackBerry device user closes the device.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Pearl Flip Series smartphone • BlackBerry Device Software 4.6
Rule introduction	• BlackBerry Enterprise Server 4.1 SP6

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 and Basic password security IT policy • Yes in all other preconfigured IT policies
Exceptions	• BlackBerry Enterprise Server for Novell GroupWiseonly with devices that are running BlackBerry Device Software 4.0 and later
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server 3.6

Force Multi Factor Authentication IT policy rule

Description	This rule specifies whether to force the use of multifactor authentication on a BlackBerry device.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server 5.0

Force Notifications for Keys with Medium Security Level IT policy rule

Description	This rule specifies whether a BlackBerry device displays notifications for private keys with a medium security level during the lifetime of the cached key. If a BlackBerry device user opens an encrypted email message, the device accesses the key store to obtain the private key to decrypt the email message.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server 5.0 SP1

Force Smart Card Reader Challenge Response while User Authentication is enabled IT policy rule

Description	This rule specifies whether a BlackBerry device user must always use the same BlackBerry Smart Card Reader or Advanced Security SD card to unlock a BlackBerry device.
Related rules	The Force Smart Card Two-Factor Authentication IT policy rule affects this rule. You must configure the Force Smart Card Two-Factor Authentication IT policy rule to Yes to use this rule.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 5.0 • BlackBerry Smart Card Reader 2.0
Rule introduction	• BlackBerry Enterprise Server 5.0 SP2

Force Smart Card Two Factor Authentication IT policy rule

Description	This rule specifies whether a BlackBerry device user must type a BlackBerry device password and the smart card password to unlock a device.
Related rules	This rule affects the Password Required IT policy rule. If you change this rule to Yes, the BlackBerry Enterprise Server automatically configures the Password Required IT policy rule to Yes in the same IT policy. You must configure the Password Required IT policy rule to Yes manually for a device that is running BlackBerry Device Software 4.2 and earlier.
Possible values	• Yes • No

Default value	• No
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise only with devices that are running BlackBerry Device Software 4.0 or later
Minimum requirements	• BlackBerry Device Software 3.6 • BlackBerry Smart Card Reader software 1.5 • BlackBerry Enterprise Server for IBM Domino 4.0 • BlackBerry Enterprise Server for Novell GroupWise 4.0
Rule introduction	• BlackBerry Enterprise Server 3.6

Force Smart Card Two Factor Challenge Response IT policy rule

Description	This rule specifies whether a BlackBerry device user must choose a smart card certificate to use with smart card two-factor authentication. This feature is designed to increase the security of smart card two-factor authentication, but when it is turned on, a BlackBerry device requires more time to unlock.
Related rules	The Password Required IT policy rule affects this rule. A device uses this rule only if you configure the Password Required IT policy rule to Yes. The Force Smart Card Two Factor Authentication IT policy rule affects this rule. A device uses this rule only if you configure the Force Smart Card Two Factor Authentication IT policy rule to Yes.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.2 • BlackBerry Smart Card Reader software 1.5
Rule introduction	• BlackBerry Enterprise Server 4.0 SP6

Key Store Password Maximum Timeout IT policy rule

Description	This rule specifies the maximum number of minutes that can elapse before the timeout period expires for the cached key store password and a BlackBerry device prompts a BlackBerry device user to type the password. The device key store is the database that stores the user's private keys. The key store uses a password to protect the user's private keys. By default, the device caches the key store password to minimize the number of key store password prompts. If you change this rule to 0, the device cannot cache the key store password and cannot reduce the number of password prompts.
Possible values	• 0 to 60 minutes
Default value	• 1 minute
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise only with devices that are running BlackBerry Device Software 4.0 or later
Minimum requirements	• BlackBerry Device Software 3.6 • BlackBerry Enterprise Server for IBM Domino 4.0 • BlackBerry Enterprise Server for Novell GroupWise 4.0
Rule introduction	• BlackBerry Enterprise Server 3.6

Lock Button Usage IT policy rule

Description	This rule specifies what happens when a user presses the lock button on a BlackBerry device. If you set this rule to Force Password Lock, the user must type their password to unlock the device. If you set this rule to Device Default, the user can unlock the keyboard and screen without typing a password.
Related rules	This rule is affected by the Password Required IT policy rule. If you set this rule to Force Password Lock, you should set the Password Required IT policy rule to Yes.
Possible values	• Force Password Lock • Device Default

Default value	• Device Default
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server 5.0 SP4

Lock on Proximity Authenticator Disconnect IT policy rule

Description	This rule specifies whether a BlackBerry device must lock either when a BlackBerry device user disconnects a proximity authenticator, such as the BlackBerry Smart Card Reader, or when a proximity authenticator is out of range of the device. This IT policy rule does not require the device to use a proximity authenticator. To require the device to use a proximity authenticator, you can configure the Force Multi Factor Authentication IT policy rule and Allowed Authentication Mechanisms IT policy rule.
Possible values	• Yes • No
Default value	• Yes in the Advanced security IT policy and Advanced security with No 3rd Party Applications IT policy • No in all other preconfigured IT policies
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server 5.0 SP1

Lock on Smart Card Removal IT policy rule

Description	This rule specifies whether a BlackBerry device locks when a BlackBerry device user removes the smart card from the BlackBerry Smart Card Reader or disconnects the BlackBerry Smart Card Reader from a device. Not all smart card reader drivers support smart card removal detection.

Related rules	This rule affects the Password Required IT policy rule. If you change this rule to Yes, the BlackBerry Enterprise Server configures the Password Required IT policy rule to Yes automatically in the same IT policy. This rule affects the Force Smart Card Two Factor Authentication IT policy rule. If you change this rule to Yes, the BlackBerry Enterprise Server configures the Force Smart Card Two Factor Authentication IT policy rule to Yes automatically in the same IT policy.
Possible values	• Yes • No
Default value	• No
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise only with devices that are running BlackBerry Device Software 4.0 or later
Minimum requirements	• BlackBerry Device Software 3.6 • BlackBerry Enterprise Server for IBM Domino 4.0 • BlackBerry Enterprise Server for Novell GroupWise 4.0
Rule introduction	• BlackBerry Enterprise Server 3.6

Login Disclaimer IT policy rule

Description	This rule specifies the disclaimer that a BlackBerry device can display before a BlackBerry device user unlocks the device for the first time after you or a user resets the device. The limit for the disclaimer is 512 characters.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server 5.0 SP1

Maximum Smart Card User Authenticator Certificate Status Check Period IT policy rule

Description	This rule specifies the maximum length of time (in minutes) that can elapse between status checks of the user authentication certificates that a BlackBerry device uses with smart cards. During each period, the device requests the status of the certificate. If the certificate is revoked, the device locks and a BlackBerry device user is unable to unlock it unless the certificate status changes from On Hold to Good.
Related rules	The Password Required IT policy rule affects this rule. The device uses this rule only if you configure the Password Required IT policy rule to Yes. The Force Smart Card User Authentication IT policy rule affects this rule. The device uses this rule only if you configure the Force Smart Card User Authentication IT policy rule to Yes. The Force Smart Card Two Factor Challenge Response IT policy affects this rule. The device uses this rule only if you configure the Force Smart Card Two Factor Challenge Response IT policy rule to Yes.
Possible values	• 240 to 40,320 minutes
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.5
Rule introduction	• BlackBerry Enterprise Server 4.1 SP5

Media Card Format on Device Wipe IT policy rule

Description	This rule specifies whether a BlackBerry device formats a media card when a BlackBerry device user or administrator deletes all data on the device permanently.
Possible values	• Allowed • Required • Disallowed

Default value	• Allowed
Minimum requirements	• BlackBerry 6
Rule introduction	• BlackBerry Enterprise Server 5.0 SP1

Message Classification IT policy rule

Description	This rule specifies the set of message classifications that are available to apply to email messages that a BlackBerry device user sends using the BlackBerry Enterprise Server.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.2
Rule introduction	• BlackBerry Enterprise Server 4.1 SP2

Message Classification Title IT policy rule

Description	This rule specifies the title of the message classification that a BlackBerry device includes when a BlackBerry device user applies the message classification to email messages.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.3
Rule introduction	• BlackBerry Enterprise Server 4.1 SP4

Minimal Encryption Key Store Security Level IT policy rule

Description	This rule specifies the minimum security level of the private key that a BlackBerry device uses to encrypt email messages. When you configure this rule, all keys must use the security level that you configure as the minimum, but a BlackBerry device user can configure a higher security level on the device.
Possible values	• Low security • Medium security • High security
Default value	• Low security
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0

Minimal Signing Key Store Security Level IT policy rule

Description	This rule specifies the minimum security level of the private key that a BlackBerry device uses to sign email messages. When you configure this rule, keys must use the security level that you configure as the minimum, but a BlackBerry device user can configure a higher security level on the device.
Possible values	• Low security • Medium security • High security
Default value	• Low security
Minimum requirements	• BlackBerry Device Software 4.0

Rule introduction	• BlackBerry Enterprise Server 4.0

Password Required for Application Download IT policy rule

Description	This rule specifies whether a BlackBerry device prompts a BlackBerry device user for the device password when using the browser to download applications.
Related rules	The Password Required IT policy rule affects this rule. The device uses this rule only if you configure the Password Required IT policy rule to Yes.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.2.2
Rule introduction	• BlackBerry Enterprise Server 4.1 SP4

Primary Transcoder IT policy rule

Description	This rule specifies the primary transcoder and its transcoding scheme. The format is: <hash> [inside|outside], [window size]], where <hash> is the hash of the primary transcoder application's eldest sibling module, and [inside|outside] indicates whether the transcoder is applied on the inside or outside. If you specify that the transcoder is outside and the device supports it, the data is encrypted using BlackBerry transport layer encryption first, and then encoded by the transcoder. If you specify that the transcoder is inside, or if the device does not support transcoding data after BlackBerry transport layer encryption is applied, the data is first encoded and then encrypted using BlackBerry transport layer encryption. The default is inside. The [window size] specifies the time delay (in minutes) after transcoding starts before non-transcoded packets are dropped. If not specified, the default value is 15 minutes.

Related rules	Security Transcoder Cod File Hashes IT policy rule affects this rule. You must specify the primary transcoder's hash in the Transcoder Cod File Hash IT Policy rule.
Default value	• Null value
Minimum requirements	• BlackBerry 7.1
Rule introduction	• BlackBerry Enterprise Server 5.0 SP4

Require Secure APB Messages IT policy rule

Description	This rule specifies whether a BlackBerry device can receive email messages that are not highly secure, including APB messages from a BlackBerry Enterprise Server.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.2
Rule introduction	• BlackBerry Enterprise Server 4.0 SP6

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 4.0 SP6

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. The previous name of this rule was Remote Wipe Reset to Factory Defaults. 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 4.1 SP4

Secure Wipe Delay After IT Policy Received IT policy rule

Description	This rule specifies the length of time that can elapse after a BlackBerry device receives an IT policy update or IT administration command that the device deletes all BlackBerry device user data. Use this rule to make the device delete the user data after a specific period of time if it cannot receive IT policy updates or IT administration commands. If you set this IT policy rule, set the Policy Resend Interval on the BlackBerry Enterprise Server to a value that is lower than this rule to prevent the device from deleting the user data unexpectedly.
Possible values	• 2 to 8760 hours
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.2
Rule introduction	• BlackBerry Enterprise Server 4.0 SP6

Secure Wipe Delay After Lock IT policy rule

Description	This rule specifies the length of time after a BlackBerry device locks that the device deletes all BlackBerry device user data. Use this rule to require that a device delete the user data if the user has not unlocked the device within the specified period of time.
Possible values	• 2 to 720 hours
Default setting	• Null value
Minimum requirements	• BlackBerry Device Software 4.2

Rule introduction	• BlackBerry Enterprise Server 4.0 SP6

Secure Wipe if Low Battery IT policy rule

Description	This rule specifies whether a BlackBerry device deletes the BlackBerry device user data if the battery power level is low enough to turn off the wireless transceiver. Use this rule to require that the device deletes the user data when the battery power level is too low to receive IT policy updates or IT administration commands.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.2
Rule introduction	• BlackBerry Enterprise Server 4.0 SP6

Security Service Colors IT policy rule

Description	This rule specifies two background colors that can display for email messages that a BlackBerry device receives. Configure the colors in red-green-blue hexadecimal format. The first color represents the background color of email messages that a device receives from the same BlackBerry Enterprise Server that sent the IT policy. The second color represents the background color of email messages that a device receives from other services (for example, the BlackBerry Internet Service). Separate multiple values with a semicolon (;).
Possible values	• 0xffffff: white • 0x000000: black • 0xff0000: red • 0x00ff00: green • 0x0000ff: blue

Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0

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 (,).
Related rules	This rule affects the Primary Transcoder IT policy rule. If you configure the Primary Transcoder rule, you must specify the primary transcoder's hash in this rule.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.5
Rule introduction	• BlackBerry Enterprise Server 4.1 SP5

Trusted Certificate Thumbprints IT policy rule

Description	This rule specifies the Hex-ASCII certificate thumbprints that are used on a BlackBerry device and are generated using the SHA-1 algorithm, MD5 algorithm, SHA-256 algorithm, or SHA-512 algorithm. Separate multiple thumbprints with semi-colons (;). If you configure this rule, a BlackBerry device user can only add certificates to the trusted key store that use the thumbprints that you specify in this rule. The SHA-256 algorithm and SHA-512 algorithm require BlackBerry Device Software 5.0 or later.
Default value	• Null value
Exceptions	• BlackBerry Enterprise Server for Novell GroupWise only with devices that are running BlackBerry Device Software 4.0 or later

Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server 3.6

Two Factor Content Protection Usage IT policy rule

Description	This rule specifies whether a BlackBerry device user can turn on two-factor content protection on a BlackBerry device. Two-factor content protection on the device is designed to protect the decryption keys for content protection with both a private key that is stored on a smart card and the device password. When a user turns on two-factor content protection, the device requires more time to unlock than if two-factor content protection is not turned on. To unlock the device, the user must have the appropriate smart card driver and a supported driver for the smart card reader installed on the device. You cannot reset the device password after you or a user turns on two-factor content protection. To restore the decryption keys for content protection and unlock the device, the user must have the smart card and must know the device password and the PIN for the smart card.
Related rules	The Content Protection Strength IT policy rule affects this rule. If you change this rule to Required, the device can use this rule only if you also configure the Content Protection Strength IT policy rule to Yes. The Force Smart Card Two Factor Authentication IT policy rule affects this rule. If you change this rule to Required, the device can use this rule only if you also change the value of the Force Smart Card Two Factor Authentication IT policy rule to Yes. The Force Smart Card Two Factor Authentication IT policy rule affects this rule. Alternatively, instead of changing the value of the Force Smart Card Two Factor Authentication IT policy rule to Yes, you can change the value of the Force Multi Factor Authentication IT policy rule to Yes and change the Allowed Authentication Mechanisms IT policy rule to use only a smart card user authenticator.
Possible values	• Allowed • Required • Disallowed
Default value	• Allowed
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server 5.0 SP1

Use Camera When Locked IT policy rule

Description	This rule specifies whether a BlackBerry device user can take pictures when the device is locked.
Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry 7.1
Rule introduction	• BlackBerry Enterprise Server 5.0 SP4 • KB34639

Use Media Controls When Locked IT policy rule

Description	This rule specifies whether a BlackBerry device user can use media controls (for example, adjust the volume) and view information about media playing on the device (for example, current song name) when the device is locked.
Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry 7.1
Rule introduction	• BlackBerry Enterprise Server 5.0 SP4 • KB34639

Weak Digest Algorithms IT policy rule

Description	This rule specifies the digest algorithms that a BlackBerry device considers weak. The device uses the list of weak digest algorithms to verify the following data: • Algorithms that are used to digitally sign email messages that the device receives are strong enough • Certificate chains for the certificates that are used to sign email messages that the device receives are strong enough • Certificates that are presented to the device from web pages that use HTTPS are strong enough If you set this rule, you can prevent the user from sending an S/MIME-encrypted message or PGP encrypted message using a certificate or key that has a corresponding public key that is weak. If you set this rule for any digest algorithm, the device considers the algorithm weak in all cases. You cannot specify SHA-384 and SHA-512 as weak algorithms.
Possible values	• MD2 • MD4 • MD5 • RIPEMD128 • RIPEMD16 • SHA • SHA224 • SHA256
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.3
Rule introduction	• BlackBerry Enterprise Server 4.1 SP5

Service Exclusivity policy group

Allow Other Browser Services IT policy rule

Description	This rule specifies whether a BlackBerry device user can use browser services other than the BlackBerry MDS Connection Service on a BlackBerry device.
Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server 3.5

Allow Other Calendar Services IT policy rule

Description	This rule specifies whether a BlackBerry device user can use calendar services other than the standard calendar application on a BlackBerry device.
Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry Device Software 4.3
Rule introduction	• BlackBerry Enterprise Server 4.1 SP5

Allow Other Message Services IT policy rule

Description	This rule specifies whether a BlackBerry device user can use email messaging services other than the BlackBerry Enterprise Server on a BlackBerry device. If you set this rule to No and apply this rule to a device that is running BlackBerry 6 or later, this rule prevents the user from sending and receiving email messages from other email messaging services on the device. If you set this rule to No and apply this rule to a device that is running BlackBerry Device Software 5.0 or earlier, this rule does not prevent the user from receiving email messages from other email messaging services on the device.
Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server 3.5

Allow Public AIM Services IT policy rule

Description	This rule specifies whether a BlackBerry device user can use AOL Instant Messenger (AIM service) on a BlackBerry device.
Possible values	• Yes • No
Default value	• Yes
Rule introduction	• BlackBerry Enterprise Server 3.6 SP6

Allow Public Google Talk Services IT policy rule

Description	This rule specifies whether a BlackBerry device user can use Google Talk on a BlackBerry device.
Possible values	• Yes • No
Default value	• Yes
Rule introduction	• BlackBerry Enterprise Server 4.0 SP4

Allow Public ICQ Services IT policy rule

Description	This rule specifies whether a BlackBerry device user can use ICQ on a BlackBerry device.
Possible values	• Yes • No
Default value	• Yes
Rule introduction	• BlackBerry Enterprise Server 3.6 SP6

Allow Public IM Services IT policy rule

Description	This rule specifies whether a BlackBerry device user can use public instant-messaging applications on a BlackBerry device. This rule applies to all public instant-messaging services for devices that were released after the introduction of this rule. To prevent a user from using Yahoo! Messenger for BlackBerry smartphones 1.0 on the device, set the Allow Public Yahoo! Messenger Services IT policy rule to No.
Possible values	• Yes • No

Default value	• Yes
Rule introduction	• BlackBerry Enterprise Server 4.0 SP4

Allow Public WLM Services IT policy rule

Description	This rule specifies whether a BlackBerry device user can use Windows Live Messenger on a BlackBerry device.
Possible values	• Yes • No
Default setting	• Yes
Rule introduction	• BlackBerry Enterprise Server 4.1 SP5

Allow Public Yahoo! Messenger Services IT policy rule

Description	This rule specifies whether a BlackBerry device user can use Yahoo! Messenger on a BlackBerry device.
Possible values	• Yes • No
Default value	• Yes
Rule introduction	• BlackBerry Enterprise Server 3.6 SP4

Allow Network Address Book Sync IT policy rule

Description	This rule specifies whether a BlackBerry device user can synchronize contacts on a BlackBerry device with the network address book that your organization's wireless service provider provides. The previous name of this rule was Allow T-Mobile Mobile Backup Contact Sync. If your organization uses T-Mobile as its wireless service provider, change the value of this rule to "Faves Only" to permit the user to synchronize only the contacts that are included in the user's MyFaves plan with the T-Mobile Mobile Backup. If your organization does not use T-Mobile as its wireless service provider and you change the value for this rule to "Faves Only", the device uses the default value for this rule instead.
Possible values	• Enabled • Disabled • Faves Only
Default value	• Disabled
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server 5.0

Smart Dialing policy group

The IT policy rules in the Smart Dialing policy group are obsolete in BlackBerry Enterprise Server 5.0 and later.

If you want to restrict outgoing calls, you can configure the can configure the Restrict Outgoing Cellular Calls IT policy rule in the Firewall policy group.

Enable Smart Dialing Policy IT policy rule

Description	This rule specifies whether smart dialing is available on a BlackBerry device.

	This rule is obsolete in BlackBerry Enterprise Server 4.1 SP4 and later and BlackBerry Device Software 4.0.2 and later.
Possible values	• Yes • No
Default setting	• Yes
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0 SP1

Set Local Area Code IT policy rule

Description	This rule specifies the local area code for phone numbers. This rule is obsolete in BlackBerry Enterprise Server 4.1 SP4 and later and BlackBerry Device Software 4.0.2 and later.
Related rules	The Enable Smart Dialing IT policy rule affects this rule. A BlackBerry device uses this rule only if you configure the Enable Smart Dialing IT policy rule to Yes.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0 SP1

Set Local Country Code IT policy rule

Description	This rule specifies the local country code for phone numbers. This rule is obsolete in BlackBerry Enterprise Server 4.1 SP4 and later and BlackBerry Device Software 4.0.2 and later.

Related rules	The Enable Smart Dialing IT policy rule affects this rule. A BlackBerry device uses this rule only if you configure the Enable Smart Dialing IT policy rule to Yes.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0 SP1

Set National Number Length IT policy rule

Description	This rule specifies the length of local phone numbers. This rule is obsolete in BlackBerry Enterprise Server 4.1 SP4 and later and BlackBerry Device Software 4.0.2 and later.
Related rules	The Enable Smart Dialing IT policy rule affects this rule. A BlackBerry device uses this rule only if you configure the Enable Smart Dialing IT policy rule to Yes.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0 SP1

Smart Dialing Allow Device Changes IT policy rule

Description	This rule specifies whether a BlackBerry device user can change the smart dialing options on a BlackBerry device. This rule is obsolete in BlackBerry Enterprise Server 4.1 SP4 and later and BlackBerry Device Software 4.2.2 and later.
Related rules	The Enable Smart Dialing IT policy rule affects this rule. The device uses this rule only if you configure the Enable Smart Dialing IT policy rule to Yes.

Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0 SP1

TCP policy group

TCP APN IT policy rule

Description	This rule specifies whether a BlackBerry device must use the default APN when the device uses TCP.
Possible values	• 0 to 120 characters
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0

TCP Password IT policy rule

Description	This rule specifies whether a BlackBerry device must use the default APN password when the device uses TCP.
Possible values	• 0 to 32 characters

Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0

TCP Username IT policy rule

Description	This rule specifies whether a BlackBerry device must use the default APN user name when the device uses TCP.
Possible values	• 0 to 32 characters
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0

TLS Application policy group

Device Side Only IT policy rule

Description	This rule specifies whether the BlackBerry Enterprise Solution permits proxy mode TLS/SSL or proxy HTTPS connections between a BlackBerry device and a BlackBerry Enterprise Server. By default, the BlackBerry Enterprise Solution permits proxy mode TLS or proxy HTTPS connections. If you set this rule to Yes, the BlackBerry device must use TLS/SSL for all HTTPS connections. If TLS/SSL is not available on the device, an exception occurs.

Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0

Disable Untrusted Connection IT policy rule

Description	This rule specifies whether to prevent a BlackBerry device from connecting to untrusted servers during TLS connections.
Possible values	• Disable untrusted connections • Allow untrusted connections • Prompt user on BlackBerry device
Default value	• Prompt user on BlackBerry device
Minimum requirements	• BlackBerry Device Software 3.6.1
Rule introduction	• BlackBerry Enterprise Server 3.6

Disable Weak Ciphers IT policy rule

Description	This rule specifies whether to prevent a BlackBerry device from using weak ciphers with TLS connections.
Possible values	• Disable weak ciphers • Allow weak ciphers • Prompt user on BlackBerry device

Default value	• Prompt user on BlackBerry device
Minimum requirements	• BlackBerry Device Software 3.6.1
Rule introduction	• BlackBerry Enterprise Server 3.6

Disable Weak Digests IT policy rule

Description	This rule specifies whether a BlackBerry device can use weak digests with TLS connections.
Possible values	• Disable weak digests • Allow weak digests • Prompt user on BlackBerry device
Default value	• Allow weak digests for devices that are running BlackBerry Device Software 4.7 or earlier • Disable weak digests for devices that are running BlackBerry Device Software 5.0 and later
Minimum requirements	• BlackBerry Device Software 4.7.1
Rule introduction	• BlackBerry Enterprise Server 5.0 SP1

Invalid Connection IT policy rule

Description	This rule specifies whether to prevent a BlackBerry device from permitting TLS connections to servers that have invalid certificates.
Possible values	• Allow invalid connections • Disallow invalid connections • Prompt user on BlackBerry device
Default value	• Prompt user on BlackBerry device

Minimum requirements	• BlackBerry Device Software 3.6.1
Rule introduction	• BlackBerry Enterprise Server 3.6

Minimum Strong DH Key Length IT policy rule

Description	This rule specifies the minimum DH key size (in bits) that a BlackBerry device can use with TLS connections. If you configure the minimum key size on the BlackBerry Enterprise Server to be greater than the minimum key size on the device, the device prompts a BlackBerry device user to trust every highly secure website that uses a key size in its certificate that is less than the minimum key size on the BlackBerry Enterprise Server. For example, if the user browses to a highly secure website that uses a 512-bit DH key in its certificate, the device prompts the user to trust the website. If the user trusts the website and selects the Don't Ask Again option, the minimum key size on the device is configured to 512 bits. If you set the minimum key size on the BlackBerry Enterprise Server to 2048 bits, the device prompts the user to trust every highly secure website that uses a key size in its certificate that is less than 2048 bits.
Possible values	• 512 to 4096 bits
Default value	• 1024 bits on the BlackBerry device • 512 bits on the BlackBerry Enterprise Server
Minimum requirements	• BlackBerry Device Software 3.6.1
Rule introduction	• BlackBerry Enterprise Server 3.6

Minimum Strong DSA Key Length IT policy rule

Description	This rule specifies the minimum DSA key size (in bits) that a BlackBerry device can use TLS connections. If you configure the minimum key size on the BlackBerry Enterprise Server to be greater than the minimum key size on the device, the device prompts a BlackBerry device user to trust every highly

	secure website that uses a key size in its certificate that is less than the minimum key size on the BlackBerry Enterprise Server. For example, if the user browses to a highly secure website that uses a 512-bit DSA key in its certificate, the device prompts the user to trust the website. If the user trusts the website and selects the Don't Ask Again option, the minimum key size on the device is configured to 512 bits. If you configure the minimum key size on the BlackBerry Enterprise Server to 1024 bits, the device prompts the user to trust every highly secure website that uses a key size in its certificate that is less than 1024 bits.
Possible values	• 512 to 1024 bits
Default value	• 1024 bits on the BlackBerry device • 512 bits on the BlackBerry Enterprise Server
Minimum requirements	• BlackBerry Device Software 3.6.1
Rule introduction	• BlackBerry Enterprise Server 3.6 SP1

Minimum Strong ECC Key Length IT policy rule

Description	This rule specifies the minimum ECC key size (in bits) that a BlackBerry device can use with TLS connections. If you configure the minimum key size on the BlackBerry Enterprise Server to be greater than the minimum key size on the device, the device prompts a BlackBerry device user to trust every highly secure website that uses a key size in its certificate that is less than the minimum key size on the BlackBerry Enterprise Server. For example, if the user browses to a highly secure website that uses a 160-bit ECC key in its certificate, the device prompts the user to trust the website. If the user trusts the website and selects the Don't Ask Again option, the minimum key size on the device is configured to 160 bits. If you configure the minimum key size on the BlackBerry Enterprise Server to 233 bits, the device prompts the user to trust every highly secure website that uses a key size in its certificate that is less than 233 bits.
Possible values	• 160 to 571 bits
Default value	• 163 bits on the BlackBerry device • 160 bits on the BlackBerry Enterprise Server

Minimum requirements	• BlackBerry Device Software 3.6.1
Rule introduction	• BlackBerry Enterprise Server 3.6

Minimum Strong RSA Key Length IT policy rule

Description	This rule specifies the minimum RSA key size (in bits) that a BlackBerry device can use with TLS connections. If you configure the minimum key size on the BlackBerry Enterprise Server to be greater than the minimum key size on the device, the device prompts the user to trust every highly secure website that uses a key size in its certificate that is less than the minimum key size on the BlackBerry Enterprise Server. For example, if the user browses to a highly secure website that uses a 512-bit RSA key in its certificate, the device prompts the user to trust the website. If the user trusts the website and selects the Don't Ask Again option, the minimum key size on the device is configured to 512 bits. If you configure the minimum key size on the BlackBerry Enterprise Server to 2048 bits, the device prompts the user to trust every highly secure website that uses a key size in its certificate that is less than 2048 bits.
Possible values	• 512 to 4096 bits
Default value	• 1000 bits on the BlackBerry device • 512 bits on the BlackBerry Enterprise Server
Minimum requirements	• BlackBerry Device Software 3.6.1
Rule introduction	• BlackBerry Enterprise Server 3.6

Prevent Insecure Renegotiation IT policy rule

Description	This rule specifies whether to prevent a BlackBerry device from opening a TLS connection to a server that does not support the TLS Renegotiation Indication Extension. If you set this rule to Yes, the device cannot connect to servers that do not use the TLS Renegotiation Indication Extension. Set this rule to Yes if you what to help protect users from possible man-in-the-middle attacks over TLS.

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

Require FIPS Ciphers IT policy rule

Description	This rule specifies whether a BlackBerry device must use FIPS-compliant algorithms with TLS connections.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 3.6.1
Rule introduction	• BlackBerry Enterprise Server 3.6

Unmatched Domain Name IT policy rule

Description	This rule specifies whether a BlackBerry device can open a TLS connection to a server that has a domain name that does not match any domain names in the server's certificate.
Possible values	• Prevent unmatched domain name • Allow unmatched domain name • Prompt user on BlackBerry device

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

User Feedback IT policy group

Allow User Feedback IT policy rule

Description	This rule specifies whether a BlackBerry device user can provide feedback to Research In Motion.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.6.1
Rule introduction	• BlackBerry Enterprise Server 5.0 SP1

VPN policy group

Disable VPN User Profiles IT policy rule

Description	This rule specifies whether a BlackBerry device user can create VPN profiles on a BlackBerry device.

Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.2.1
Rule introduction	• BlackBerry Enterprise Server 4.1 SP3

Enable VPN IT policy rule

Description	This rule specifies whether the VPN client on a BlackBerry device is turned on. This rule is obsolete in BlackBerry Enterprise Server 4.1 SP3 and later.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0 SP1

Use VPN Xauth IT policy rule

Description	This rule specifies whether a VPN client on a BlackBerry device should use Xauth certificates to authenticate with your organization's VPN gateway.
Related rules	The Enable VPN IT policy rule affects this rule. You must change the Enable VPN IT policy rule to Yes so that the device can use this rule.
Possible values	• Yes

	• No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0 SP1

VPN Allow Handheld Changes IT policy rule

Description	This rule specifies whether a BlackBerry device user can change all VPN IT policy rules on a BlackBerry device. This rule is obsolete in BlackBerry Enterprise Server 4.1 SP3 and later.
Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0 SP1

VPN Allow Password Save IT policy rule

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

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

VPN Disable Prompt for Credentials Re-Entry IT policy rule

Description	This rule specifies whether a BlackBerry device turns off the prompt for a BlackBerry device user to type the VPN credentials after the user tries to authenticate to the VPN server but is not successful.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.2.1
Rule introduction	• BlackBerry Enterprise Server 4.1 SP3

VPN DNS Configuration IT policy rule

Description	This rule specifies your organization's VPN DNS configuration.
Related rules	The Enable VPN IT policy rule affects this rule. You must configure the Enable VPN IT policy rule to Yes so that a BlackBerry device can use this rule.
Possible values	• Yes • No
Default value	• Yes

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

VPN Domain Name IT policy rule

Description	This rule specifies the suffix for your organization's domain name using the FQDN format.
Related rules	The Enable VPN IT policy rule affects this rule. You must configure the Enable VPN IT policy rule to Yes so that a BlackBerry device can use this rule. The VPN DNS Configuration IT policy rule affects this rule. You must configure the VPN DNS Configuration IT policy rule to No so that a device can use this rule.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0 SP1

VPN Gateway Address IT policy rule

Description	This rule specifies the IP address or FQDN of your organization's VPN server.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0 SP1

VPN Group Name IT policy rule

Description	This rule specifies the group name of your organization's VPN server. Specify the group name of your organization's VPN server only if the VPN client requires it.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0 SP1

VPN Group Password IT policy rule

Description	This rule 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 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0 SP1

VPN IKE Cipher IT policy rule

Description	This rule specifies the encryption algorithm that a BlackBerry device uses to authenticate the IKE exchanges. Change the value only if the encryption algorithm does not support AES-128.
Possible values	• DES • 3DES • AES128 • AES192

	• AES256
Default value	• AES128
Minimum requirements	• BlackBerry Device Software 4.0.0
Rule introduction	• BlackBerry Enterprise Server 4.0 SP1

VPN IKE DH Group IT policy rule

Description	This rule specifies the DH group that a BlackBerry device uses to generate key material. Change the value only if the DH group does not use ECC.
Related rules	The Enable VPN IT policy rule affects this rule. You must configure the Enable VPN IT policy rule to Yes so that a device can use this rule.
Possible values	• Group 1 • Group 2 • Group 5 • Group 7 • Group 9
Default value	• Group 7
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0 SP1

VPN IKE Hash IT policy rule

Description	This rule specifies the keyed-hash method authentication code that a BlackBerry device can use. Change the value only if the hash method authentication code does not support SHA-1 160 bits.

Possible values	• MD-5 128 bits • SHA-1 160 bits
Default value	• SHA-1 160 bits
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0 SP1

VPN IPSec Cipher and Hash IT policy rule

Description	This rule specifies the encryption algorithm and hash that a BlackBerry device uses for IPSec Security Associations. Change the value only if the IPSec cipher and hash are not AES-128 and SHA-1.
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 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0 SP1

VPN Minimal Certificate Encryption Key Security Level IT policy rule

Description	This rule specifies the minimum security level for private keys that a BlackBerry device uses for authentication methods that require client certificates.
Possible values	• High security • Medium security • Low security
Default value	• Low security
Minimum requirements	• BlackBerry Device Software 4.2.2
Rule introduction	• BlackBerry Enterprise Server 4.1 SP4

VPN NAT Keep Alive IT policy rule

Description	This rule specifies the NAT keep-alive frequency. Specify the interval that must elapse before 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 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0 SP1

VPN Password Hidden on Input IT policy rule

Description	This rule specifies whether a BlackBerry device displays asterisks (*) instead of characters when a BlackBerry device user types a VPN password.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.2.1
Rule introduction	• BlackBerry Enterprise Server 4.1 SP3

VPN PFS IT policy rule

Description	This rule specifies whether Perfect Forward Secrecy is turned on for a BlackBerry device. Change the value only if your organization does not support Perfect Forward Secrecy.
Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0 SP1

VPN Primary DNS IT policy rule

Description	This rule specifies the static setting for the IP address of your organization's primary DNS server.
Related rules	The Enable VPN IT policy rule affects this rule. You must change the Enable VPN IT policy rule to Yes so that a BlackBerry device can use this rule. The VPN DNS Configuration IT policy rule affects this rule. You must change the VPN DNS Configuration IT policy rule to No so that the device can use this rule.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0 SP1

VPN Secondary DNS IT policy rule

Description	This rule specifies the static setting for the IP address of your organization's secondary DNS server.
Related rules	The Enable VPN IT policy rule affects this rule. You must change the Enable VPN IT policy rule to Yes so that a BlackBerry device can use this rule. The VPN DNS Configuration IT policy rule affects this rule. You must change the VPN DNS Configuration IT policy rule to No so that the device can use this rule.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0 SP1

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.
Related rules	The Enable VPN IT policy rule affects this rule. You must change the Enable VPN IT policy rule to Yes so that a device can use this rule.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0 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.
Related rules	The Enable VPN IT policy rule affects this rule. You must change the Enable VPN IT policy rule to Yes so that a device can use this rule.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0 SP1

VPN Vendor Type IT policy rule

Description	This rule specifies the type of VPN client that the VPN client on a BlackBerry device emulates.
Related rules	The Enable VPN IT policy rule affects this rule. You must change the Enable VPN IT policy rule to Yes so that a device can use this rule.
Possible values	• Alcatel 7130 Secure VPN Gateway Family • Avaya VSU Series • Check Point 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 3100 Series • Lucent Firewall Brick Family • Netscreen Systems • Nortel Networks Contivity VPN Switch Series • ReefEdge Connect Server • Secure Computing Sidewinder Firewall • Symantec Raptor Firewall and PowerVPN
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0 SP1

VPN Xauth Type IT policy rule

Description	This rule specifies the type of BlackBerry device user authentication that your organization's VPN server uses.
Related rules	The Enable VPN IT policy rule affects this rule. You must change the Enable VPN IT policy rule to Yes so that a BlackBerry device can use this rule.
Possible values	• User name and password required • SecurID required
Default value	• User name and password required
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0 SP1

Visual Voice Mail policy group

Allow Users to Save Messages IT policy rule

Description	This rule specifies whether a BlackBerry device user can use visual voice mail to save or forward voice mail messages.
Related rules	The Disable Visual Voice Mail IT policy rule affects this rule. If you want to permit a user access to visual voice mail, you must change the Disable Visual Voice Mail IT policy rule to No.
Possible values	• Yes • No
Default value	• Yes

Minimum requirements	• BlackBerry Device Software 4.5
Rule introduction	• BlackBerry Enterprise Server 5.0

Disable Visual Voice Mail IT policy rule

Description	This rule specifies whether to permit a BlackBerry device user access to visual voice mail. If a wireless service provider gives the user access to visual voice mail, it might prevent the user from receiving standard voice mail notifications.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.5
Rule introduction	• BlackBerry Enterprise Server 5.0

Password Complexity IT policy rule

Description	This rule specifies the minimum password length that a BlackBerry device user is required to type to access the TUI.
Related rules	This rule affects the Password Required IT policy rule. If you configure this rule, you must change the Password Required IT policy rule to Yes.
Possible values	• 0 to 16 digits
Default value	• 4 digits
Minimum requirements	• BlackBerry Device Software 4.5

Rule introduction	• BlackBerry Enterprise Server 5.0

Require Password IT policy rule

Description	This rule specifies whether a BlackBerry device user must type a password to access the TUI.
Possible value	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.5
Rule introduction	• BlackBerry Enterprise Server 5.0

WTLS Application policy group

Invalid Connection IT policy rule

Description	This rule specifies whether a BlackBerry device can connect to servers with invalid certificates during WTLS connections.
Possible values	• Disallow invalid connections • Allow invalid connections • Prompt user on BlackBerry device
Default value	• Prompt user on BlackBerry device
Minimum requirements	• BlackBerry Device Software 3.6

Rule introduction	• BlackBerry Enterprise Server 3.6

Minimum Strong DH Key Length IT policy rule

Description	This rule specifies the minimum DH key size (in bits) that a BlackBerry device can use with WTLS connections. This rule is obsolete in BlackBerry Enterprise Server 5.0 SP2.
Possible values	• 512 to 4096 bits
Default value	• 1024 bits on the device • 512 bits on the BlackBerry Enterprise Server
Minimum requirements	• BlackBerry Device Software 3.6 • BlackBerry Enterprise Server 3.6
Rule introduction	• BlackBerry Enterprise Server 3.6

Minimum Strong ECC Key Length IT policy rule

Description	This rule specifies the minimum ECC key size (in bits) that a BlackBerry device can use with WTLS connections. This rule is obsolete in BlackBerry Enterprise Server 5.0 SP2.
Possible values	• 160 to 571 bits
Default value	• 163 bits on the device • 160 bits on the BlackBerry Enterprise Server
Minimum requirements	• BlackBerry Device Software 3.6

Rule introduction	• BlackBerry Enterprise Server 3.6

Minimum Strong RSA Key Length IT policy rule

Description	This rule specifies the minimum RSA key size (in bits) that a BlackBerry device can use with WTLS connections. This rule is obsolete in BlackBerry Enterprise Server 5.0 SP2.
Possible values	• 512 to 4096 bits
Default value	• 1000 bits on the device • 512 bits on the BlackBerry Enterprise Server
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server 3.6

Require FIPS Ciphers IT policy rule

Description	This rule specifies whether a BlackBerry must use FIPS-compliant algorithms with WTLS connections.
Possible values	• False • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0

Untrusted Connections IT policy rule

Description	This rule specifies whether to a BlackBerry can connect to untrusted servers during WTLS connections.
Possible values	• Disallow untrusted connections • Allow untrusted connections • Prompt user on BlackBerry device
Default value	• Prompt user on BlackBerry device
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server 3.6

Weak Ciphers IT policy rule

Description	This rule specifies whether a BlackBerry device can use weak ciphers with WTLS connections.
Possible values	• Disallow weak ciphers • Allow weak ciphers • Prompt user on BlackBerry device
Default value	• Prompt user on BlackBerry device
Minimum requirements	• BlackBerry Device Software 3.6
Rule introduction	• BlackBerry Enterprise Server 3.6

Wi-Fi policy group

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

Allow Mobile Hotspot Mode IT policy rule

Description	This rule specifies whether to allow Mobile Hotspot mode on a BlackBerry device.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry 7.1
Rule introduction	• BlackBerry Enterprise Server 5.0 SP4 • KB28284

BlackBerry Infrastructure Wi-Fi Access Mode IT policy rule

Description	This rule specifies whether a BlackBerry device can connect to the BlackBerry Infrastructure over a Wi-Fi network to access the BlackBerry Enterprise Server or BlackBerry Internet Service. You can override this rule using the Wi-Fi configuration setting that is named Wi-Fi BlackBerry Infrastructure Wi-Fi Access Mode. You can use this setting to configure the access mode for a specific Wi-Fi network, and you can use this rule to configure the access mode for other Wi-Fi networks. If you turn off access to the BlackBerry Infrastructure over the Wi-Fi network using this rule, you cannot override this rule using the configuration setting. The previous name of this rule was BlackBerry Infrastructure WLAN Access Mode.

Possible values	• Access requires VPN • Access does not require VPN • Access disabled
Default value	• Access does not require VPN
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server 5.0 • KB19406

Blocked Wi-Fi SSIDs IT policy rule

Description	This rule specifies whether to prevent a BlackBerry device user from adding Wi-Fi profiles for SSIDs that you specify to a BlackBerry device. Specify a list of Wi-Fi SSIDs, separated by commas (,), that you do not want the device to associate with. The previous name of this rule was Blocked WLAN SSIDs.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server 5.0 • KB19406

Disable Data Exchange for Mobile Hotspot Mode IT policy rule

Description	This rule specifies whether Wi-Fi enabled devices can exchange data when they are connected to a BlackBerry device in Mobile Hotspot mode.

Related rules	The Allow Mobile Hotspot Mode IT policy rule affects this rule. The device uses this rule only when you set the Allow Mobile Hotspot Mode IT policy rule to Yes.
Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry 7.1
Rule introduction	• BlackBerry Enterprise Server 5.0 SP4 • KB28284

Disable Enterprise Wi-Fi Profiles Backup IT policy rule

Description	This rule specifies whether Wi-Fi profile configuration information is included when a BlackBerry device user backs up the device data using BlackBerry Desktop Software, BlackBerry Web Desktop Manager, or automatic wireless backup. If you set this rule to Yes, Wi-Fi profile configuration information is not included when the user backs up the device data.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry 7
Rule introduction	• BlackBerry Enterprise Server 5.0 SP4 • KB28284

Disable GAN-Only Mode IT policy rule

Description	This rule specifies whether a BlackBerry device user can select the GAN-only mode from the list of GAN selection modes on a BlackBerry device.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.2.1
Rule introduction	• BlackBerry Enterprise Server 4.1 SP3

Disable GAN-Preferred Mode IT policy rule

Description	This rule specifies whether a BlackBerry device user can select the GAN-preferred mode from the list of GAN selection modes on a BlackBerry device.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.2.1
Rule introduction	• BlackBerry Enterprise Server 4.1 SP3

Disable GAN Selection Mode Editing IT policy rule

Description	This rule specifies whether a BlackBerry device user can change the GAN selection mode on a BlackBerry device.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.2.1
Rule introduction	• BlackBerry Enterprise Server 4.1 SP3

Disable WAN-Only Mode IT policy rule

Description	This rule specifies whether a BlackBerry device user can select the WAN-only mode from the list of GAN selection modes on a BlackBerry device.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.2.1
Rule introduction	• BlackBerry Enterprise Server 4.1 SP3

Disable WAN-Preferred Mode IT policy rule

Description	This rule specifies whether a BlackBerry device user can select the WAN-preferred mode from the list of GAN selection modes on a BlackBerry device.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.2.1
Rule introduction	• BlackBerry Enterprise Server 4.1 SP3

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. The previous name of this rule was Disable WLAN.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.2.1
Rule introduction	• BlackBerry Enterprise Server 4.1 SP3

Disable Wi-Fi Direct Access to BlackBerry Enterprise Server IT policy rule

Description	This rule specifies whether a BlackBerry device can connect to the BlackBerry Enterprise Server using a Wi-Fi connection. The previous name of this rule was Disable WLAN Direct Access to BlackBerry Enterprise Server.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.2.1
Rule introduction	• BlackBerry Enterprise Server 4.1 SP3

Disable Wi-Fi User Profiles IT policy rule

Description	This rule specifies whether a BlackBerry device user can create Wi-Fi profiles on a BlackBerry device. The previous name of this rule was Disable WLAN User Profiles.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.2.1
Rule introduction	• BlackBerry Enterprise Server 4.1 SP3

GAN Signal Quality Threshold IT policy rule

Description	This rule specifies the signal quality threshold that a BlackBerry device uses to change from the WAN to the GAN. In WAN-preferred mode, if the signal quality drops below the threshold, the device tries to transition to the GAN. The signal quality is related to the bit error rate and is described in the 3GPP 5.08 8.2.4 specification as follows: • 0 = good quality • 7 = worst quality
Possible values	• 0 to 7
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.2.1
Rule introduction	• BlackBerry Enterprise Server 4.1 SP3

GAN Signal Strength Threshold IT policy rule

Description	This rule specifies the signal strength threshold that a BlackBerry device can use to change from the WAN to the GAN. In the WAN-preferred mode, if the signal strength drops below the threshold, the device tries to transition to GAN. This signal strength is specified in Received Signal Level units and is described in the 3GPP 5.08 8.1.4 specification as follows: • 0 = -111 dBm • 63 = -48 dBm
Possible values	• 0 to 63
Default value	• Null value

Minimum requirements	• BlackBerry Device Software 4.2.1
Rule introduction	• BlackBerry Enterprise Server 4.1 SP3

GAN Wi-Fi Threshold IT policy rule

Description	This rule specifies the threshold for the Wi-Fi signal quality that a BlackBerry device uses to change from the GAN to the WAN. If the Wi-Fi signal quality drops below the threshold in the GAN-preferred mode and an acceptable cell is available, the device tries to change from the GAN to the WAN. The previous name of this rule was GAN WLAN Threshold.
Possible values	• Low • Medium • High
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.2.1
Rule introduction	• BlackBerry Enterprise Server 4.1 SP3

Override Hotspot APN Information IT policy rule

Description	This rule specifies the hotspot APN information that overrides the hotspot APN information set by the wireless service provider in the service record. Specify the APN information in a comma-separated list including login type, APN, user name, and password.
Default value	• Null value
Minimum requirements	• BlackBerry 7.1

Rule introduction	• BlackBerry Enterprise Server 5.0 SP4 • KB29510

Prohibited SSIDs for Mobile Hotspot Mode IT policy rule

Description	This rule specifies a list of SSIDs that a BlackBerry device cannot use as Mobile Hotspot SSIDs. Separate multiple SSIDs with a comma (,).
Related rules	The Allow Mobile Hotspot Mode IT policy rule affects this rule. The device uses this rule only when you set the Allow Mobile Hotspot Mode IT policy rule to Yes.
Default value	• Null value
Minimum requirements	• BlackBerry 7.1
Rule introduction	• BlackBerry Enterprise Server 5.0 SP4 • KB28284

Wi-Fi Allow Handheld Changes IT policy rule

Description	This rule specifies whether BlackBerry devices users can change all Wi-Fi policy rules on their BlackBerry devices. The previous name of this rule was WLAN Allow Handheld Changes.
Possible values	• Yes • No
Default values	• Yes in the Default IT policy • No in all other preconfigured IT policies
Minimum requirements	• BlackBerry Device Software 4.0

Rule introduction	• BlackBerry Enterprise Server 4.0 SP1

Wi-Fi Default Gateway IT policy rule

Description	This rule 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. The previous name of this rule was WLAN Default Gateway.
Related rules	The Wi-Fi DHCP Configuration IT policy rule affects this rule. If you configure the value for the Wi-Fi DHCP Configuration IT policy rule to Yes, do not change the value for this rule to Yes.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0 SP1

Wi-Fi Default KEY ID IT policy rule

Description	This rule specifies the default WEP key ID. Verify that the WEP key ID matches the WEP access point ID and the corresponding WEP key. The previous name of this rule was WLAN Default KEY ID.
Possible values	• 1 to 4
Default value	• 1
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0 SP1

Wi-Fi DHCP Configuration IT policy rule

Description	This rule specifies whether your organization uses DHCP for dynamic network configuration. If you use a Wi-Fi network that includes subnets, turn on DHCP to permit roaming between subnets. The previous name of this rule was WLAN DHCP Configuration.
Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0 SP1

Wi-Fi Disable Prompt for Credentials Re-Entry IT policy rule

Description	This rule specifies whether a BlackBerry device turns off the prompt for a BlackBerry device user to re-type the Wi-Fi credentials after authentication is not successful. The previous name of this rule was WLAN Disable Prompt for Credentials Re-Entry.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.2.1
Rule introduction	• BlackBerry Enterprise Server 4.1 SP3

Wi-Fi Enable Authentication Page IT policy rule

Description	This rule specifies whether the Wi-Fi Login browser is available on a BlackBerry 7270 smartphone. The previous name of this rule was WLAN Enable Authentication Page. This rule is obsolete in BlackBerry Enterprise Server 4.1 SP4 and later.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0 SP1

Wi-Fi IP Address IT policy rule

Description	This rule specifies the IP address (for example, 10.0.0.1) that a BlackBerry device can use if DHCP on the device is turned off. The previous name of this rule was WLAN IP Address.
Related rules	The Wi-Fi DHCP Configuration IT policy rule affects this rule. A device uses this rule only if you change the Wi-Fi DHCP Configuration IT policy rule to No. If you change the Wi-Fi DHCP Configuration IT policy rule to Yes, do not change this rule to Yes.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0 SP1

Wi-Fi Internet Access Path IT policy rule

Description	This rule specifies how a BlackBerry device must access the Internet when the device uses Wi-Fi profiles that are not configured for your organization.
Possible values	• Access through BlackBerry MDS Connection Service • Access through Wi-Fi
Default value	• Access through Wi-Fi
Minimum requirements	• BlackBerry 6
Rule introduction	• BlackBerry Enterprise Server 5.0 SP3

Wi-Fi Link Security IT policy rule

Description	This rule specifies the type of security that a BlackBerry device requires to access a Wi-Fi network. It controls Wi-Fi profiles specified in IT Policy. It does not control WLAN profiles assigned in BlackBerry Administration Service or associations with scanned networks.
Possible values	• Open Wi-Fi security • WEP • PSK • EAP-PEAP • EAP-LEAP • EAP-TLS
Default value	• Open Wi-Fi security
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0 SP1

Wi-Fi Minimal EAP-TLS Certificate Encryption Key Security Level IT policy rule

Description	This rule specifies the minimum security level for a private key that an EAP authentication method (for example, EAP-TLS) uses with a client certificate. The previous name of this rule was WLAN Minimal EAP-TLS Certificate Encryption Key Security Level. This rule is obsolete in BlackBerry Enterprise Server 4.1 SP4 and later.
Possible values	• High security • Medium security • Low security
Default value	• Low security
Minimum requirements	• BlackBerry Device Software 4.0.1
Rule introduction	• BlackBerry Enterprise Server 4.0 SP1

Wi-Fi Password Hidden on Input IT policy rule

Description	This rule specifies whether the password for Wi-Fi authentication is represented by asterisks (*) as the BlackBerry device user types it. The previous name of this rule was WLAN Password Hidden on Input.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.2.1

Rule introduction	• BlackBerry Enterprise Server 4.1 SP3

Wi-Fi Preshared Key IT policy rule

Description	This rule specifies the PSK if your organization uses PSK to authenticate to a Wi-Fi network. The previous name of this rule was WLAN Preshared Key.
Related rules	The Wi-Fi Link Security IT policy rule affects this rule. A BlackBerry device uses this rule only if you configure the Wi-Fi Link Security IT policy rule to PSK.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0 SP1

Wi-Fi Primary DNS IT policy rule

Description	This rule 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. The previous name of this rule was WLAN Primary DNS.
Related rules	The Wi-Fi DHCP Configuration IT policy rule affects this rule. The device uses this rule only if you change the Wi-Fi DHCP Configuration IT policy rule to No. If you change the Wi-Fi DHCP Configuration IT policy rule to Yes, do not change this rule to Yes.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0 SP1

Wi-Fi Profile Forwarding Mode IT policy rule

Description	This rule specifies whether a BlackBerry device user can forward the Wi-Fi profiles that the user creates on a BlackBerry device to another BlackBerry device using an email message, PIN message, SMS text message, or BlackBerry Messenger message, with or without a password. You cannot resend an IT policy to forward Wi-Fi profiles. The previous name of this rule was WLAN profile forwarding mode.
Related rules	The Allow Peer-to-Peer Messages IT policy rule affects this rule. A user can forward a Wi-Fi profile using a PIN message only if you change the Allow Peer-to-Peer Messages IT policy rule to Yes. The Allow SMS IT policy rule affects this rule. A user can forward a Wi-Fi profile using a SMS text message only if you change the Allow SMS IT policy rule to Yes. The Disable BlackBerry Messenger IT policy rule affects this rule. A user can forward a Wi-Fi profile using BlackBerry Messenger only if you change the Disable BlackBerry Messenger IT policy rule to No. The Firewall Block Incoming Messages IT policy rule affects this rule. A user can forward a Wi-Fi profile using a PIN message, an SMS message, or BlackBerry Messenger only if the Firewall Block Incoming Messages IT policy rule does not prevent the device from processing PIN messages, SMS messages, or BlackBerry Messenger messages.
Possible values	• Enabled • Enabled with a forwarding password • Disabled
Default value	• Enabled
Minimum requirements	• BlackBerry Device Software 5.0 • BlackBerry Smart Card Reader 2.0
Rule introduction	• BlackBerry Enterprise Server 5.0 • KB19406

Wi-Fi Secondary DNS IT policy rule

Description	This rule 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. The previous name of this rule was WLAN Secondary DNS.
Related rules	The Wi-Fi DHCP Configuration IT policy rule affects this rule. The device uses this rule only if you change the Wi-Fi DHCP Configuration IT policy rule to No. If you change the Wi-Fi DHCP Configuration IT policy rule to Yes, do not change this rule to Yes.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0 SP1

Wi-Fi SSID IT policy rule

Description	This rule specifies the network name of the Wi-Fi network and its wireless access points. The SSID is case-sensitive and has a maximum length of 32 characters. You must change the value before a BlackBerry device can access the Wi-Fi network. The previous name of this rule was WLAN SSID.
Possible values	• 0 to 32 characters
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0 SP1

Wi-Fi Subnet Mask IT policy rule

Description	This rule 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. The previous name of this rule was WLAN Subnet Mask.
Related rules	The Wi-Fi DHCP Configuration IT policy rule affects this rule. The device uses this rule only if you change the Wi-Fi DHCP Configuration IT policy rule to No. If you change the Wi-Fi DHCP Configuration IT policy rule to Yes, do not change this rule to Yes.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0 SP1

Wi-Fi User Name IT policy rule

Description	This rule specifies the user name for PEAP security access or LEAP security access on a BlackBerry device. Configure a value if you want to create a default value for all BlackBerry device users. If the user types a user name on a device manually, IT policy updates overwrite or delete the value that the user types. To retain the value that the user specifies on the device, verify that the updated IT policy uses the same value as the IT policy on the device. The previous name of this rule was WLAN User Name.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0 SP1

Wi-Fi User Password IT policy rule

Description	This rule specifies the password for PEAP security access or LEAP security access on a BlackBerry device. Configure a value if you want to create a default value for all BlackBerry device users. If the user types a password on a device manually, any IT policy updates overwrite or delete the value that the user types. To retain the value that the user specifies on the device, verify that the updated IT policy uses the same value as the IT policy on the device. The previous name of this rule was WLAN User Password.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0 SP1

Wi-Fi WEP Key 1 IT policy rule

Description	This rule specifies the password for WEP key 1 using the format xx:xx:xx:xx:xx. This rule supports 5 or 13 pairs of hexadecimal digits (0 to 9 and A to F) separated by a colon (:). For example, AB:CD:EF:01:23 or AB:CD:EF:01:23:45:67:89:AB:CD:EF:01:23. The previous name of this rule was WLAN WEP Key 1.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0 SP1

Wi-Fi WEP Key 2 IT policy rule

Description	This rule specifies the password for WEP key 2 using the format xx:xx:xx:xx:xx. This rule supports 5 or 13 pairs of hexadecimal digits (0 to 9 and A to F) separated by a colon (:). For example, AB:CD:EF:01:23 or AB:CD:EF:01:23:45:67:89:AB:CD:EF:01:23. The previous name of this rule was WLAN WEP Key 2.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0 SP1

Wi-Fi WEP Key 3 IT policy rule

Description	This rule specifies the password for WEP key 3 using the format xx:xx:xx:xx:xx. This rule supports 5 or 13 pairs of hexadecimal digits (0 to 9 and A to F) separated by a colon (:). For example, AB:CD:EF:01:23 or AB:CD:EF:01:23:45:67:89:AB:CD:EF:01:23. The previous name of this rule was WLAN WEP Key 3.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0 SP1

Wi-Fi WEP Key 4 IT policy rule

Description	This rule specifies the password for WEP key 4 using the format xx:xx:xx:xx:xx. This rule supports 5 or 13 pairs of hexadecimal digits (0 to 9 and A to F) separated by a colon (:). For example, AB:CD:EF:01:23 or AB:CD:EF:01:23:45:67:89:AB:CD:EF:01:23.

	The previous name of this rule was WLAN WEP Key 4.
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0 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.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 5.0
Rule introduction	• BlackBerry Enterprise Server 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 5.0 SP1 • KB19406

Wireless Software Upgrades policy group

Allow Non Enterprise Upgrade IT policy rule

Description	This rule specifies whether to permit Research In Motion or a wireless service provider to request that a BlackBerry device download updates for the BlackBerry Device Software over the wireless network. The BlackBerry Administration Service changes the value for this rule to the default value and does not display this rule when you configure the BlackBerry Administration Service to display the BlackBerry Device Software pages. For more information, see the *BlackBerry Device Software Update Guide*.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.5

Rule introduction	• BlackBerry Enterprise Server 4.1 SP4

Allow Wireless Security Updates IT policy rule

Description	This rule specifies whether a BlackBerry device can download updates for the BlackBerry Device Software over the wireless network that Research In Motion or a wireless service provider makes available. An update is considered a security-related update if it has a securityfixlevel value of 1 to 4. This rule does not control whether the device can download the updates over the wireless network that you make available using the BlackBerry Administration Service.
Possible values	• Accept All • Accept Security Updates Only • Accept None
Default value	• Accept All
Minimum requirements	• BlackBerry 6
Rule introduction	• BlackBerry Enterprise Server 5.0 SP3 • KB23515

Disallow Device User Requested Rollback IT policy rule

Description	This rule specifies whether to prevent a BlackBerry device user from returning to a previous version of the BlackBerry Device Software after the user updates the BlackBerry Device Software over the wireless network. The BlackBerry Administration Service changes the value for this rule to Yes and does not display this rule when you configure the BlackBerry Administration Service to display the BlackBerry Device Software pages.
Possible values	• Yes • No
Default value	• No

Minimum requirements	• BlackBerry Device Software 4.5
Rule introduction	• BlackBerry Enterprise Server 4.1 SP4

Disallow Device User Requested Upgrade IT policy rule

Description	This rule specifies whether to prevent a BlackBerry device user from requesting available updates for the BlackBerry Device Software over the wireless network. The BlackBerry Administration Service changes the value for this rule to Yes and does not display this rule when you configure the BlackBerry Administration Service to display the BlackBerry Device Software pages. For more information, see the *BlackBerry Device Software Update Guide*.
Possible value	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.5
Rule introduction	• BlackBerry Enterprise Server 4.1 SP4

Disallow Patch Download Over International 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 internationally.
Possible values	• Yes • No
Default value	• No

Minimum requirements	• BlackBerry Device Software 4.5
Rule introduction	• BlackBerry Enterprise Server 4.1 SP4

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.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.5
Rule introduction	• BlackBerry Enterprise Server 4.1 SP4

Disallow Patch Download Over WAN IT policy rule

Description	This rule specifies whether to prevent a BlackBerry device from downloading updates for the BlackBerry Device Software over a WAN connection.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.5

Rule introduction	• BlackBerry Enterprise Server 4.1 SP4

Disallow Patch Download Over Wi-Fi IT policy rule

Description	This rule specifies whether to prevent a BlackBerry device from downloading updates for the BlackBerry Device Software over a Wi-Fi connection.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.5
Rule introduction	• BlackBerry Enterprise Server 4.1 SP4

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 • BlackBerry Enterprise Server 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 • BlackBerry Enterprise Server 4.1 SP2

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 • BlackBerry Enterprise Server 4.1 SP3

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. This configuration setting is obsolete in BlackBerry Enterprise Server 4.1 SP3.
Possible values	• Yes • No
Default value	• Yes
Minimum requirements	• BlackBerry Device Software 4.0 • BlackBerry Enterprise Server 4.0 SP1

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 • BlackBerry Enterprise Server 4.1 SP3

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 • BlackBerry Enterprise Server 4.1 SP4

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 InfrastructureWi-Fi Access Mode IT policy rule. When you change this setting, you override the BlackBerry InfrastructureWi-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 InfrastructureWi-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 InfrastructureWi-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 • BlackBerry Enterprise Server 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 • BlackBerry Enterprise Server 4.1 SP2

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 • BlackBerry Enterprise Server 4.0 SP1

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 • BlackBerry Enterprise Server 4.1 SP2

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 • BlackBerry Enterprise Server 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 • BlackBerry Enterprise Server 4.1 SP3

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 • BlackBerry Enterprise Server 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. This setting is obsolete in BlackBerry Enterprise Server 4.1 SP4 and later.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.0 • BlackBerry Enterprise Server 4.0 SP1

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 • BlackBerry Enterprise Server 4.1 SP3

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 • BlackBerry Enterprise Server 4.1 SP3

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
Rule introduction	• BlackBerry Enterprise Server 5.0.3

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 • BlackBerry Enterprise Server 4.1 SP2

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 • BlackBerry Enterprise Server 4.0 SP1

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 • BlackBerry Enterprise Server 4.0 SP1

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 • BlackBerry Enterprise Server 4.0 SP1

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 • BlackBerry Enterprise Server 4.1 SP2

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 • BlackBerry Enterprise Server 4.1 SP3

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 • BlackBerry Enterprise Server 4.1 SP3

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 • BlackBerry Enterprise Server 4.1 SP3

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 • BlackBerry Enterprise Server 4.1 SP2

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

	• BlackBerry Enterprise Server 4.1 SP3

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 • BlackBerry Enterprise Server 4.1 SP3

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 • BlackBerry Enterprise Server 4.0 SP1

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

	• BlackBerry Enterprise Server 4.1 SP2

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 • BlackBerry Enterprise Server 4.1 SP3

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 • BlackBerry Enterprise Server 4.0 SP1

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 • BlackBerry Enterprise Server 4.1 SP2

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 • BlackBerry Enterprise Server 4.0 SP1

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 • BlackBerry Enterprise Server 4.0 SP1

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 • BlackBerry Enterprise Server 4.0 SP1

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 • BlackBerry Enterprise Server 4.0 SP1

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 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. This configuration setting is obsolete in BlackBerry Enterprise Server 4.1 SP3 and later.
Possible values	• Yes • No
Default value	• No
Minimum requirements	• BlackBerry Device Software 4.2
Rule introduction	• BlackBerry Enterprise Server 4.1 SP2

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
Rule introduction	• BlackBerry Enterprise Server 5.0.1

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 • BlackBerry Enterprise Server 4.1 SP3

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 • BlackBerry Enterprise Server 4.1 SP2

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 • BlackBerry Enterprise Server 4.0 SP1

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 • BlackBerry Enterprise Server 4.1 SP2

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 • BlackBerry Enterprise Server 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 • BlackBerry Enterprise Server 4.1 SP2

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 • BlackBerry Enterprise Server 4.1 SP2

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 • BlackBerry Enterprise Server 4.1 SP2

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 • BlackBerry Enterprise Server 4.1 SP2

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

	• BlackBerry Enterprise Server 4.1 SP2

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 • BlackBerry Enterprise Server 4.1 SP3

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 • BlackBerry Enterprise Server 4.1 SP2

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 • BlackBerry Enterprise Server 4.1 SP2

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 • BlackBerry Enterprise Server 4.1 SP2

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 • BlackBerry Enterprise Server 4.1 SP3

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 • BlackBerry Enterprise Server 4.1 SP2

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. This rule is obsolete in BlackBerry Enterprise Server 4.1 SP4.
Possible values	• Low security • High security • Medium security
Default value	• Low security
Minimum requirements	• BlackBerry Device Software 4.2.1 • BlackBerry Enterprise Server 4.1 SP3

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 • BlackBerry Enterprise Server 4.1 SP2

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 • BlackBerry Enterprise Server 4.1 SP2

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 • BlackBerry Enterprise Server 4.1 SP2

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 • BlackBerry Enterprise Server 4.1 SP3

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 • BlackBerry Enterprise Server 4.1 SP3

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 • BlackBerry Enterprise Server 4.1 SP2

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
Rule introduction	• BlackBerry Enterprise Server 5.0.1

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
Rule introduction	• BlackBerry Enterprise Server 5.0.1

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
Rule introduction	• BlackBerry Enterprise Server 5.0.1

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
Rule introduction	• BlackBerry Enterprise Server 5.0.1

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
Rule introduction	• BlackBerry Enterprise Server 5.0.1

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
Rule introduction	• BlackBerry Enterprise Server 5.0.1

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 • BlackBerry Enterprise Server 4.1 SP3

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 • BlackBerry Enterprise Server 4.1 SP3

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 • BlackBerry Enterprise Server 4.1 SP2

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 • BlackBerry Enterprise Server 4.1 SP2

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 Series • Check Point 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 3100 Series • Lucent Firewall Brick Family

	• Netscreen Systems • Nortel Networks Contivity VPN Switch Series • ReefEdge Connect Server • Secure Computing Sidewinder Firewall • Symantec Raptor Firewall and PowerVPN
Default value	• Null value
Minimum requirements	• BlackBerry Device Software 4.2 • BlackBerry Enterprise Server 4.1 SP2

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 • BlackBerry Enterprise Server 4.1 SP2

Application control policy rules 6

For information about configuring application control policy rules, see the *BlackBerry Enterprise Server 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 4.0

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 4.0

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 4.0

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 • BlackBerry Enterprise Server 5.0
Rule introduction	• BlackBerry Enterprise Server 5.0

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 5.0

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 5.0 SP2

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 4.0

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 4.0

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 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 4.0

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 4.0

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 5.0

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 4.1 SP2

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.
Related rules	The Minimal Signing Key Store Security Level IT policy rule affects this rule. If you configure the Minimal Signing Key Store Security Level IT policy rule to use the high-security level, this rule does not apply. The device prompts a BlackBerry device user for the key-store password each time that an application tries to access the private key. The Minimal Encryption Key Store Security Level IT policy rule affects this rule. If you configure the Minimal Encryption Key Store Security Level IT policy rule to use the high-security level, this rule does not apply. The device prompts the user for the key store password each time that an application tries to access the private key.
Possible values	• Disallowed • Allowed
Default value	• Allowed
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0

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 4.0

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 5.0

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

Description	This rule specifies whether an application can add, change, or delete .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 5.0

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 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 4.0

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 4.0

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 5.0

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 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.
Related rules	The Disable Serial Port Profile IT policy rule affects this rule. If you configure the Disable Serial Port Profile IT policy rule to Yes, this rule does not apply. A BlackBerry device cannot use the Bluetooth SPP to establish a serial connection to a Bluetooth enabled device.
Possible values	• Disallowed • Allowed
Default value	• Allowed
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0

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 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 4.1 SP2

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 5.0

Is Key Store Medium Security Allowed application control policy rule

Description	This rule specifies whether an application can access key-store items that are stored at the medium security level. The application must prompt a BlackBerry device user for the key-store password when it tries to access the private key for the first time or when the private key password timeout expires.
Related rules	The Minimal Signing Key Store Security Level IT policy rule affects this rule. If you configure the Minimal Signing Key Store Security Level IT policy rule to use the high security level, a BlackBerry device does not use this rule. The device prompts the user for the key-store password each time that an application tries to access the private key. The Minimal Encryption Key Store Security Level IT policy rule affects this rule. If you configure the Minimal Encryption Key Store Security Level IT policy rule to use the high security level, the device does not use this rule. The device prompts the user for the key-store password each time that an application tries to access the private key.
Possible values	• Disallowed • Allowed
Default value	• Allowed
Minimum requirements	• BlackBerry Device Software 4.0
Rule introduction	• BlackBerry Enterprise Server 4.0

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 5.0 SP2

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 5.0 SP2

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 4.1 SP2

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 4.0

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 4.0

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 4.0

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 when the user inserts it in the holster.	Force Lock When Holstered	Security policy group	Yes
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
Protect the device transport key on a locked device.	Force Content Protection of Master Key	Security	Yes
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 services that your organization can monitor.	Allow Other Browser Services	Service Exclusivity	No
	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

Glossary

8

A2DP	Advanced Audio Distribution Profile
AES	Advanced Encryption Standard
APB	all points bulletin
API	application programming interface
APN	access point name
ASCII	American Standard Code for Information Interchange
AVRCP	Audio/Video Remote Control Profile
BCC	blind carbon copy
BIP	Bearer Independent Protocol
BlackBerry MDS	BlackBerry Mobile Data System
BSM	browser session manager
CAST	Computer Assisted Seriation Test
CHAP	Challenge Handshake Authentication Protocol
COM	Component Object Model
CRL	certificate revocation list
DES	Data Encryption Standard
DH	Diffie-Hellman
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DSA	Digital Signature Algorithm
DTMF	Dual Tone Multi-Frequency
DUN	Dial-up Networking
EAP	Extensible Authentication Protocol
EAP-FAST	Extensible Authentication Protocol Flexible Authentication via Secure Tunneling

EAP-LEAP	Extensible Authentication Protocol Lightweight Extensible Authentication Protocol
EAP-TLS	Extensible Authentication Protocol Transport Layer Security
EAP-TTLS	Extensible Authentication Protocol Tunneled Transport Layer Security
ECC	Elliptic Curve Cryptography
FIPS	Federal Information Processing Standards
FQDN	fully qualified domain name
FTP	File Transfer Protocol
GAN	generic access network
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
HFP	Hands-Free Profile
HSP	Headset Profile
HTML	Hypertext Markup Language
HTTPS	Hypertext Transfer Protocol over Secure Sockets Layer
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IMEI	International Mobile Equipment Identity
IOT	interoperability test
IP	Internet Protocol
IPsec	Internet Protocol Security
IT	information technology
LED	light-emitting diode
MAP	Message Access Profile
MDS	Mobile Data System
MFH	message from handheld
MMS	Multimedia Messaging Service

MTH	message to handheld
NAT	network address translation
NFC	Near Field Communication
OBEX	Object Exchange
PAC	proxy auto-configuration
PEAP	Protected Extensible Authentication Protocol
PFS	Perfect Forward Secrecy
PIM	personal information management
PIN	personal identification number
PKI	Public Key Infrastructure
PSK	pre-shared key
RC	Rivest's Cipher
RNG	random number generator
SAN	subject alternative name
SHA	Secure Hash Algorithm
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
S/MIME	Secure Multipurpose Internet Mail Extensions
SMS	Short Message Service
SPP	Serial Port Profile
SSID	service set identifier
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TUI	telephone UI
UID	unique identifier
UPnP	Universal Plug and Play
USB	Universal Serial Bus
VPN	virtual private network
WAN	wide area network

WAP	Wireless Application Protocol
WEP	Wired Equivalent Privacy
WLAN	wireless local area network
WTLS	Wireless Transport Layer Security
xAuth	Extended Authentication

Legal notice

9

QUALITY, NON-INFRINGEMENT, SATISFACTORY QUALITY, OR TITLE, OR ARISING FROM A STATUTE OR CUSTOM OR A COURSE OF DEALING OR USAGE OF TRADE, OR RELATED TO THE DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN, ARE HEREBY EXCLUDED. YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY BY STATE OR PROVINCE. SOME JURISDICTIONS MAY NOT ALLOW THE EXCLUSION OR LIMITATION OF IMPLIED WARRANTIES AND CONDITIONS. TO THE EXTENT PERMITTED BY LAW, ANY IMPLIED WARRANTIES OR CONDITIONS RELATING TO THE DOCUMENTATION TO THE EXTENT THEY CANNOT BE EXCLUDED AS SET OUT ABOVE, BUT CAN BE LIMITED, ARE HEREBY LIMITED TO NINETY (90) DAYS FROM THE DATE YOU FIRST ACQUIRED THE DOCUMENTATION OR THE ITEM THAT IS THE SUBJECT OF THE CLAIM.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, IN NO EVENT SHALL BLACKBERRY 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 BLACKBERRY PRODUCTS OR SERVICES, DOWNTIME COSTS, LOSS OF THE USE OF BLACKBERRY 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 BLACKBERRY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, BLACKBERRY 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 BLACKBERRY AND ITS AFFILIATED COMPANIES, THEIR SUCCESSORS, ASSIGNS, AGENTS, SUPPLIERS (INCLUDING AIRTIME SERVICE PROVIDERS), AUTHORIZED BLACKBERRY 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 BLACKBERRY OR ANY AFFILIATES OF BLACKBERRY 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 BlackBerry'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 BlackBerry'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 BlackBerry and BlackBerry 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 BlackBerry.

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

BlackBerry Limited
2200 University Avenue East
Waterloo, Ontario
Canada N2K 0A7

BlackBerry UK Limited
200 Bath Road
Slough, Berkshire SL1 3XE
United Kingdom

Published in Canada