

# BlackBerry Enterprise Server

Version: 4.1

## Policy Reference Guide



# Contents

<b>1</b>	<b>IT policy rules</b>	<b>14</b>
	Using the BlackBerry Professional Software	14
	New IT policy rules in this release	14
	Policy precedence on the BlackBerry device	15
	Understanding IT policy rule names and policy group names	15
	Setting IT policy rules	15
	Where to find descriptions of Wi-Fi IT policy rules	16
	Using IT policy rules on other devices	16
	Importing IT policy rules without the required minimum BlackBerry Enterprise Server software	16
<b>2</b>	<b>Descriptions of IT policy rules</b>	<b>17</b>
	Application Center policy group	17
	Disable Application Center IT policy rule	17
	Disable Carrier Directory IT policy rule	17
	BlackBerry Messenger policy group	18
	Disable BlackBerry Messenger IT policy rule	18
	Disallow Forwarding Of Contacts IT policy rule	18
	Messenger Audit Email Address IT policy rule	18
	Messenger Audit Max Report Interval IT policy rule	19
	Messenger Audit Report Interval IT policy rule	19
	Messenger Audit UID IT policy rule	20
	BlackBerry Smart Card Reader policy group	20
	Disable Auto Reconnect To BlackBerry Smart Card Reader IT policy rule	20
	Force Erase All Keys on BlackBerry Disconnected Timeout IT policy rule	21
	Force Erase Key on PC Standby IT policy rule	21
	Maximum BlackBerry Disconnected Timeout IT policy rule	22
	Maximum BlackBerry Bluetooth Traffic Inactivity Timeout IT policy rule	22
	Maximum BlackBerry Long Term Timeout IT policy rule	23
	Maximum Bluetooth Encryption Key Regeneration Period IT policy rule	24
	Maximum Bluetooth Range IT policy rule	24
	Maximum Connection Heartbeat Period IT policy rule	25
	Maximum Number of BlackBerry Transactions IT policy rule	25
	Maximum Number of PC Pairings IT policy rule	26
	Maximum PC Bluetooth Traffic Inactivity Timeout IT policy rule	27

Maximum Number of PC Transactions IT policy rule.....	27
Maximum PC Disconnected Timeout IT policy rule.....	28
Maximum PC Long Term Timeout IT policy rule.....	28
Maximum Smart Card Not Present Timeout IT policy rule.....	29
BlackBerry Unite policy group.....	30
Disable Download Manager IT policy rule.....	30
Disable Unite! Applications IT policy rule.....	30
Bluetooth policy group.....	30
Allow Outgoing Calls IT policy rule.....	30
Disable Address Book Transfer IT policy rule.....	31
Disable Advanced Audio Distribution Profile IT policy rule.....	31
Disable Audio/Video Remote Control Profile IT policy rule.....	32
Disable Bluetooth IT policy rule.....	32
Disable Desktop Connectivity IT policy rule.....	32
Disable Dial-Up Networking IT policy rule.....	33
Disable Discoverable Mode IT policy rule.....	33
Disable File Transfer IT policy rule.....	34
Disable Handsfree Profile IT policy rule.....	34
Disable Headset Profile IT policy rule.....	34
Disable Pairing IT policy rule.....	35
Disable Serial Port Profile IT policy rule.....	35
Disable SIM Access Profile IT policy rule.....	36
Disable Wireless Bypass IT policy rule.....	36
Force CHAP Authentication on Bluetooth Link IT Policy rule.....	37
Limit Discoverable Time IT policy rule.....	37
Minimum Encryption Key Length IT policy rule.....	37
Require Encryption IT policy rule.....	38
Require LED Connection Indicator IT policy rule.....	38
Require Password for Discoverable Mode IT policy rule.....	39
Require Password for Enabling Bluetooth Support IT policy rule.....	39
Browser policy group.....	39
Allow Application Download Services IT policy rule.....	39
Allow Hotspot Browser IT policy rule.....	40
Allow IBS Browser IT policy rule.....	40
Disable Auto Synchronization in Browser IT policy rule.....	41

Disable JavaScript in Browser IT policy rule.....	41
Download Images URL IT policy rule.....	42
Download Themes URL IT policy rule.....	42
Download Tunes URL IT policy rule.....	42
MDS Browser BSM Enabled IT policy rule.....	43
MDS Browser Domains IT policy rule.....	43
MDS Browser HTML Tables Enabled IT policy rule.....	44
MDS Browser JavaScript Enabled IT policy rule.....	44
MDS Browser Style Sheets Enabled IT policy rule.....	44
MDS Browser Title IT policy rule.....	45
MDS Browser Use Separate Icon IT policy rule.....	45
Camera policy group.....	46
Disable Photo Camera IT policy rule.....	46
Disable Video Camera IT policy rule.....	46
Certificate Synchronization policy group.....	46
Random Source URL IT policy rule.....	47
User Can Disable Automatic RNG Initialization IT policy rule.....	47
Common policy group.....	47
BlackBerry Server version IT policy rule.....	47
Confirm On Send IT policy rule.....	48
Disable Kodiak PTT IT policy rule.....	49
Disable MMS IT policy rule.....	49
Disable Voice-Activated Dialing IT policy rule.....	49
Disable Voice Note Recording IT policy rule.....	50
IT Policy Notification IT policy rule.....	50
Lock Owner Info IT policy rule.....	51
Set Owner Info IT policy rule.....	51
Set Owner Name IT policy rule.....	52
Desktop Only items.....	53
Auto Backup Enabled IT policy rule.....	53
Auto Backup Exclude Messages IT policy rule.....	53
Auto Backup Exclude Sync IT policy rule.....	54
Auto Backup Frequency IT policy rule.....	54
Auto Backup Include All IT policy rule.....	55
Disable Wireless Calendar IT policy rule.....	55

Do Not Save Sent Messages IT policy rule.....	56
Force Load Count IT policy rule.....	56
Force Load Message IT policy rule.....	57
Forward Messages In Cradle IT policy rule.....	58
Message Conflict Mailbox Wins IT policy rule.....	58
Message Prompt IT policy rule.....	59
Show Application Loader IT policy rule.....	59
Show Web Link IT policy rule.....	60
Synchronize Messages Instead Of Importing IT policy rule.....	60
Web Link Label IT policy rule.....	61
Web Link URL IT policy rule.....	61
Desktop policy group.....	62
Desktop Allow Desktop Add-ins IT policy rule.....	62
Desktop Allow Device Switch IT policy rule.....	62
Desktop Password Cache Timeout IT policy rule.....	63
Disable Check For Updates Link IT policy rule.....	63
Disable Media Manager IT policy rule.....	64
Override Check For Updates URL IT policy rule.....	64
Device IOT Application policy group.....	64
Device Diagnostic App Disable IT policy rule.....	64
Set Diagnostic Report Email Address IT policy rule.....	65
Set Diagnostic Report PIN Address IT policy rule.....	65
Device Only Items.....	66
Allow BCC Recipients IT policy rule.....	66
Allow Peer-to-Peer Messages IT policy rule.....	66
Allow SMS IT policy rule.....	67
Default Browser Config UID IT policy rule.....	67
Enable Long-Term Timeout IT policy rule.....	68
Enable WAP Config IT policy rule.....	69
Home Page Address IT policy rule.....	69
Maximum Password Age IT policy rule.....	70
Home Page Address Is Read-Only IT policy rule.....	71
Maximum Security Timeout IT policy rule.....	71
Minimum Password Length IT policy rule.....	72
Password Pattern Checks IT policy rule.....	72

Password Required IT policy rule.....	73
User Can Change Timeout IT policy rule.....	74
User Can Disable Password IT policy rule.....	74
Documents To Go policy group.....	75
Disable Documents To Go IT policy rule.....	75
Hide Documents To Go Communication Menus IT policy rule.....	75
Hide Documents To Go Premium Feature Menus IT policy rule.....	76
Email Messaging policy group.....	76
Allow Auto Attachment Download IT policy rule.....	76
Attachment Viewing IT policy rule.....	77
Disable Form Submission IT policy rule.....	77
Disable Manual Download of External Images IT policy rule.....	78
Disable Notes Native Encryption Forward And Reply IT policy rule.....	78
Disable Rich Content Email IT policy rule.....	79
Enable Wireless Message Reconciliation IT policy rule.....	79
Inline Content Requests IT policy rule.....	80
Keep Message Duration IT policy rule.....	80
Keep Saved Message Duration IT policy rule.....	81
Maximum Native Attachment MFH attachment size IT policy rule.....	81
Maximum Native Attachment MFH total attachment size IT policy rule.....	81
Notes Native Encryption Password Timeout IT policy rule.....	82
Prepend Disclaimer IT policy rule.....	82
Maximum Native Attachment MTH attachment size.....	83
Enterprise Voice Client policy group.....	83
Disable DTMF Fallback IT policy rule.....	83
Disable Enterprise Voice Client IT policy rule.....	84
Lock Outgoing Line IT policy rules.....	84
Reject Non-Enterprise Voice Calls IT policy rule.....	84
Firewall policy group.....	85
Restrict Incoming Cellular Calls IT policy rule.....	85
Restrict Outgoing Cellular Calls IT policy rule.....	85
Global items.....	86
Allow Browser IT policy rule.....	86
Allow Phone IT policy rule.....	87
Auto Signature IT policy rule.....	87

Instant Messaging policy group.....	88
Disallow File Transfer Types IT policy rule.....	88
Disable Emailing Conversation IT policy rule.....	88
Disable Saving Conversation IT policy rule.....	89
Location Based Services policy group.....	89
Disable BlackBerry Maps IT policy rule.....	89
Enable Enterprise Location Tracking IT policy rule.....	89
Enterprise Location Tracking User Prompt Message IT policy rule.....	90
Enterprise Location Tracking Interval IT policy rule.....	90
MDS Integration Service policy group.....	91
Disable Activation With Public BlackBerry MDS Integration Service IT policy rule.....	91
Disable MDS Runtime IT policy rule.....	91
Disable User-Initiated Activation With Public BlackBerry MDS Integration Service IT policy rule.....	91
Lowest BlackBerry MDS Integration Service Security version Allowed IT policy rule.....	92
Verify BlackBerry MDS Integration Service Certificate IT policy rule.....	92
Memory Cleaner policy group.....	93
Force Memory Clean When Holstered IT policy rule.....	93
Force Memory Clean When Idle IT policy rule.....	93
Memory Cleaner Maximum Idle Time IT policy rule.....	94
On-Device Help policy group.....	95
On-Device Help Links IT policy rule.....	95
On-Device Help Group Label IT policy rule.....	95
Password policy group.....	96
Duress Notification Address IT policy rule.....	96
Forbidden Passwords IT policy rule.....	96
Maximum Password History IT policy rule.....	97
Periodic Challenge Time IT policy rule.....	97
Set Maximum Password Attempts IT policy rule.....	98
Set Password Timeout IT policy rule.....	99
Suppress Password Echo IT policy rule.....	99
PIM Synchronization policy group.....	100
Disable Address Wireless Synchronization IT policy rule.....	100
Disable All Wireless Synchronization IT policy rule.....	100
Disable Calendar Wireless Synchronization IT policy rule.....	101
Disable Enterprise Activation Progress IT policy rule.....	101

Disable Memopad Wireless Sync IT policy rule.....	102
Disable Phone Call Log Wireless Synchronization IT policy rule.....	102
Disable PIN Messages Wireless Synchronization IT policy rule.....	102
Disable SMS Messages Wireless Sync IT policy rule.....	103
Disable Task Wireless Sync IT policy rule.....	103
Disable Wireless Bulk Loads IT policy rule.....	104
PGP Application policy group.....	105
PGP Allowed Content Ciphers IT policy rule.....	105
PGP Allowed Encrypted Attachment Mode.....	106
PGP Allowed Encryption Type IT policy rule.....	106
PGP Blind Copy Address IT policy rule.....	106
PGP Force Digital Signature IT policy rule.....	107
PGP Force Encrypted Messages IT policy rule.....	107
PGP Minimum Strong DH Key Length IT policy rule.....	108
PGP Minimum Strong DSA Key Length IT policy rule.....	108
PGP Minimum Strong RSA Key Length IT policy rule.....	109
PGP Universal Enrollment Method IT policy rule.....	109
PGP Universal Policy Cache Timeout IT policy rule.....	110
PGP Universal Server Address IT policy rule.....	110
RIM Value-Added Applications policy group.....	111
Disable BlackBerry Wallet IT policy rule.....	111
Disable Ecommerce Content Optimization Engine IT policy rule.....	111
Disable Lotus Connections IT policy rule.....	112
Lotus Connections Activities Server IT policy rule.....	112
Lotus Connections Blogs Server IT policy rule.....	112
Lotus Connections Communities Server IT policy rule.....	113
Lotus Connections Dogear Server IT policy rule.....	113
Lotus Connections Profiles Server IT policy rule.....	114
S/MIME Application policy group.....	114
Entrust Messaging Server (EMS) Email Address IT policy rule.....	114
S/MIME Allowed Content Ciphers IT policy rule.....	115
S/MIME Allowed Encrypted Attachment Mode IT policy rule.....	115
S/MIME Allowed Encryption Types IT policy rule.....	116
S/MIME Blind Copy Address IT policy rule.....	116
S/MIME Force Digital Signature IT policy rule.....	117

S/MIME Force Encrypted Messages IT policy rule.....	117
S/MIME Force Smartcard Use IT policy rule.....	118
S/MIME Minimum Strong DH Key Length IT policy rule.....	118
S/MIME Minimum Strong ECC Key Length IT policy rule.....	119
S/MIME Minimum Strong DSA Key Length IT policy rule.....	119
S/MIME Minimum Strong RSA Key Length IT policy rule.....	120
Secure Email policy group.....	120
Canonical Certificate Domain Name IT policy rule.....	120
Disable Certificate Address Checks IT policy rule.....	121
Security policy group.....	121
Allow External Connections IT policy rule.....	121
Allow Internal Connections IT policy rule.....	122
Allow Outgoing Call When Locked IT policy rule.....	122
Allow Resetting of Idle Timer IT policy rule.....	123
Allow Screen Shot Capture IT policy rule.....	123
Allow Smart Card Password Caching IT policy rule.....	123
Allow Split-Pipe Connections IT policy rule.....	124
Allow Third Party Apps to Use Persistent Store IT policy rule.....	125
Allow Third Party Apps to Use Serial Port IT policy rule.....	125
Certificate Status Maximum Expiry Time IT policy rule.....	125
Content Protection Strength IT policy rule.....	126
Desktop Backup IT policy rule.....	127
Disable 3DES Transport Crypto IT policy rule.....	127
Disable Cut/Copy/Paste IT policy rule.....	128
Disable External Memory IT policy rule.....	128
Disable Forwarding Between Services IT policy rule.....	128
Disable Geo-Tagging of Photos IT policy rule.....	129
Disable GPS IT policy rule.....	129
Disable Invalid Certificate Use IT policy rule.....	130
Disable IP Modem IT policy rule.....	130
Disable Key Store Backup IT policy rule.....	131
Disable Key Store Low Security IT policy rule.....	131
Disable Media Manager FTP Access.....	132
Disable Message Normal Send IT policy rule.....	132
Disable Peer-to-Peer Normal Send IT policy rule.....	133

Disable Persisted Plain Text IT policy rule.....	134
Disable Public Photo Sharing Applications IT policy rule.....	134
Disable Public Social Networking Applications IT policy rule.....	134
Disable Radio When Cradled IT policy rule.....	135
Disable Revoked Certificate Use IT policy rule.....	135
Disable Smart Password Entry IT policy rule.....	136
Disable Stale Certificate Status Checks IT policy rule.....	136
Disable Stale Status Use IT policy rule.....	137
Disable Untrusted Certificate Use IT policy rule.....	137
Disable Unverified Certificate Use IT policy rule.....	138
Disable Unverified CRLs IT policy rule.....	138
Disable USB Mass Storage IT policy rule.....	139
Disable Weak Certificate Use IT policy rule.....	139
Disallow Third Party Application Downloads IT policy rule.....	140
External File System Encryption Level IT policy rule.....	141
FIPS Level IT policy rule.....	142
Firewall Block Incoming Messages IT policy rule.....	143
Firewall Whitelist Addresses IT policy rule.....	143
Force Content Protection Of Master Keys IT policy rule.....	144
Force Include Address Book In Content Protection IT policy rule.....	144
Force LED Blinking When Microphone Is On IT policy rule.....	145
Force Lock When Holstered IT policy rule.....	145
Force Smart Card Two Factor Authentication IT policy rule.....	145
Force Smart Card Two Factor Challenge Response IT policy rule.....	146
Key Store Password Maximum Timeout IT policy rule.....	147
Lock on Smart Card Removal IT policy rule.....	147
Maximum Smart Card User Authenticator Certificate Status Check Period IT policy rule.....	148
Message Classification IT policy rule.....	149
Message Classification Title IT policy rule.....	149
Minimal Encryption Key Store Security Level IT policy rule.....	149
Minimal Signing Key Store Security Level IT policy rule.....	150
Password Required for Application Download IT policy rule.....	151
Required Password Pattern IT policy rule.....	151
Remote Wipe Reset to Factory Defaults IT policy rule.....	152
Require Secure APB Messages IT policy rule.....	152

Secure Wipe Delay After IT Policy Received IT policy rule.....	153
Secure Wipe Delay After Lock IT policy rule.....	153
Secure Wipe if Low Battery IT policy rule.....	154
Security Service Colors IT policy rule.....	154
Security Transcoder Cod File Hashes IT policy rule.....	155
Trusted Certificate Thumbprints IT policy rule.....	155
Weak Digest Algorithms IT policy rule.....	156
Service Exclusivity policy group.....	156
Allow Other Browser Services IT policy rule.....	156
Allow Other Calendar Services IT policy rule.....	157
Allow Other Message Services IT policy rule.....	157
Allow Public AIM Services IT policy rule.....	158
Allow Public Google Talk Services IT policy rule.....	158
Allow Public ICQ Services IT policy rule.....	159
Allow Public IM Services IT policy rule.....	159
Allow Public WLM Services IT policy rule.....	160
Allow Public Yahoo! Messenger Services IT policy rule.....	160
SIM Application Toolkit policy group.....	160
Disable Network Location Query IT policy rule.....	160
Disable SIM Call Control IT policy rule.....	161
Disable SIM Originated Calls IT policy rule.....	161
Smart Dialing policy group.....	162
Enable Smart Dialing Policy IT policy rule.....	162
Set Local Area Code IT policy rule.....	162
Set Local Country Code IT policy rule.....	163
Set National Number Length IT policy rule.....	163
Smart Dialing Allow Device Changes IT policy rule.....	164
TCP policy group.....	164
TCP APN IT policy rule.....	164
TCP Password IT policy rule.....	165
TCP Username IT policy rule.....	165
TLS policy group.....	166
TLS Device Side Only IT policy rule.....	166
TLS Disable Invalid Connection IT policy rule.....	166
TLS Disable Untrusted Connection IT policy rule.....	167

TLS Disable Weak Ciphers IT policy rule.....	167
TLS Minimum Strong DH Key Length IT policy rule.....	167
TLS Minimum Strong DSA Key Length IT policy rule.....	168
TLS Minimum Strong ECC Key Length IT policy rule.....	169
TLS Minimum Strong RSA Key Length IT policy rule.....	169
TLS Restrict FIPS Ciphers IT policy rule.....	170
Wireless Software Upgrades policy group.....	170
Allow Non Enterprise Upgrade IT policy rule.....	170
Disallow Device User Requested Rollback IT policy rule.....	171
Disallow Device User Requested Upgrade.....	171
Disallow Patch Download Over International Roaming WAN IT policy rule.....	171
Disallow Patch Download Over Roaming WAN IT policy rule.....	172
Disallow Patch Download Over WAN IT policy rule.....	172
Disallow Patch Download Over WiFi IT policy rule.....	173
WTLS policy group.....	173
WTLS Disable Invalid Connection IT policy rule.....	173
WTLS Disable Untrusted Connection IT policy rule.....	173
WTLS Disable Weak Ciphers IT policy rule.....	174
WTLS Minimum Strong DH Key Length IT policy rule.....	174
WTLS Minimum Strong ECC Key Length IT policy rule.....	175
WTLS Minimum Strong RSA Key Length IT policy rule.....	176
WTLS Restrict FIPS Ciphers IT policy rule.....	176
<b>3 Application control policy rules.....</b>	<b>178</b>
Understanding application control policies.....	178
Setting application control policy rules.....	178
<b>4 Descriptions of application control policy rules.....</b>	<b>179</b>
Security Data application control policy rule.....	179
BlackBerry Device Keystore Medium Security application control policy rule.....	179
Bluetooth Serial Profile application control policy rule.....	180
Browser Filter Domains application control policy rule.....	180
Browser Filters application control policy rule.....	180
Device GPS application control policy rule.....	181
Disposition application control policy rule.....	181
Event Injection application control policy rule.....	182

External Domains application control policy rule.....	182
External Network Connections application control policy rule.....	182
Internal Domains application control policy rule.....	183
Internal Network Connections application control policy rule.....	183
Cross Application Communication application control policy rule.....	183
Local Connections application control policy rule.....	184
Message Access application control policy rule.....	184
Phone Access application control policy rule.....	184
Organizer Data Access application control policy rule.....	185
Themes application control policy rule.....	185
User Authenticator application control policy rule.....	186
<b>5 BlackBerry MDS Services policy rules.....</b>	<b>187</b>
Configuring how users access and use BlackBerry MDS Runtime Applications.....	187
<b>6 Descriptions of BlackBerry MDS Services policy rules.....</b>	<b>188</b>
Allow Runtime Upgrade By User BlackBerry MDS Services rule.....	188
Allow Discovery by User BlackBerry MDS Services rule.....	188
Allow Application Install by User BlackBerry MDS Services rule.....	188
Allow Push Application Install BlackBerry MDS Services rule.....	189
Allow Application Delete by User BlackBerry MDS Services rule.....	189
Allow External Access BlackBerry MDS Services rule.....	189
Allow Access to Multiple Domains BlackBerry MDS Services rule.....	190
Queue Limit for Inbound Application Messages BlackBerry MDS Services rule.....	190
Queue Limit for Outbound Application Messages BlackBerry MDS Services rule.....	191
<b>7 Examples of security policy goals.....</b>	<b>192</b>
Defining acceptable use of passwords and passphrases on BlackBerry devices.....	193
Defining measures to protect BlackBerry devices from unauthorized use.....	194
Defining the encryption strength that the BlackBerry device uses to protect data.....	194
Restricting unsecured messaging.....	195
Defining measures to prevent threats from viruses and malicious users.....	195
Limiting the resources that third-party applications installed on BlackBerry devices can access.....	196
Limiting user control of third-party applications on BlackBerry devices.....	197
Preventing RIM value-added applications from running on BlackBerry devices.....	197
Example application control policies.....	199

Blocking all third-party applications.....	199
Block all third-party applications.....	199
Permitting specific third-party applications.....	199
Permit a specific third-party application while blocking all other third-party applications.....	200
Controlling the behavior of third-party applications.....	200
Assign a default application control policy to control the behavior of allowed third-party applications.....	200
<b>8 Legal notice.....</b>	<b>201</b>

# IT policy rules

1

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

For more information about how to create an IT policy, configure an IT policy rule, and assign an IT policy to a user account or group, see the *BlackBerry Enterprise Server Administration Guide*.

## Using the BlackBerry Professional Software

If you are using the BlackBerry® Professional Software, consider BlackBerry® Enterprise Server to mean BlackBerry Professional Software in the descriptions for all IT policy rules and application control policy rules that the BlackBerry Professional Software supports.

## New IT policy rules in this release

Policy group	Rule	BlackBerry Device Software (minimum requirement)
Application Center	Disable Application Center	4.7
Application Center	Disable Carrier Directory	4.7
BlackBerry® Messenger	Disallow Forwarding of Contacts	4.6
BlackBerry Unite!	Disable BlackBerry Unite! Applications	4.2.2
BlackBerry Unite!	Disable Download Manager	4.2.2
Bluetooth	Disable SIM Access Profile	4.6
Browser	Allow Hotspot Browser	4.6
Instant Messaging	Disallow File Transfer Types	4.2
Instant Messaging	Disable Emailing Conversation	4.1
Instant Messaging	Disable Saving Conversation	4.2
PGP Application	PGP Allowed Encryption Types	4.6
RIM Value-Added Applications	Disable BlackBerry Wallet	—
RIM Value-Added Applications	Disable Lotus Connections	—
RIM Value-Added Applications	Lotus Connections Activities Server	—

Policy group	Rule	BlackBerry Device Software (minimum requirement)
RIM Value-Added Applications	Lotus Connections Profiles Blogs Server	—
RIM Value-Added Applications	Lotus Connections Communities Server	—
RIM Value-Added Applications	Lotus Connections Dogear Server	—
RIM Value-Added Applications	Lotus Connections Profiles Server	—
RIM Value-Added Applications	Disable Ecommerce Content Optimization Engine	—
RIM Value-Added Applications	Disable RIM Value-Added Applications	—
S/MIME Application	S/MIME Allowed Encryption Types	4.6

For information about adding new IT policy rules to a BlackBerry® Enterprise Server version that is earlier than the minimum requirement, visit [www.blackberry.com/btsc](http://www.blackberry.com/btsc) to read article KB05439.

## Policy precedence on the BlackBerry device

IT policy rule settings override application control policy rule settings. For example, if you change the Allow Internal Connections IT policy rule to No for BlackBerry® devices, and if these devices have an application control policy set that allows a specific application to make internal connections, the application cannot make internal connections.

The BlackBerry device revokes an application control policy and resets if the permissions of the application it is applied to become more restrictive. On supported BlackBerry devices, users can make application permissions more, but never less, restrictive than what the BlackBerry® Enterprise Server administrator sets.

## Understanding IT policy rule names and policy group names

You can use IT policy rules to control BlackBerry® devices and BlackBerry® Desktop Software in your organization's environment.

IT policy rules appear in the BlackBerry Administration Service in policy groups. Each policy group contains rules that can control common properties or applications on BlackBerry devices. The names of most IT policy rules indicate how you can use the rules to change the default behavior of the BlackBerry device and BlackBerry Desktop Software.

## Setting IT policy rules

You can assign IT policy rules to satisfy your organization's security policy requirements and to reflect the needs of the users who are assigned to that IT policy. For example, you can create an IT policy, set the IT policy rules for executive-level feature and security requirements, add executives to a group, and assign the IT policy to the group.

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

## Where to find descriptions of Wi-Fi IT policy rules

You can set VPN and WLAN IT policy rules in configuration profiles to configure your enterprise Wi-Fi network solution to support Wi-Fi® enabled BlackBerry® devices. For more information, see the *BlackBerry Enterprise Server Wi-Fi Implementation Supplement*.

## Using IT policy rules on other devices

A device that is running BlackBerry® Connect™ software or BlackBerry® Built-In™ software can use all the IT policy rules that are associated with the supported features of the BlackBerry Connect software or BlackBerry Built-In software. The BlackBerry Connect software or BlackBerry Built-In software ignores IT policy rules that are associated with unsupported features.

Although the BlackBerry Connect software or BlackBerry Built-In software might support an IT policy rule, the device that it is running on might not. For more information, contact your organization's device supplier.

Devices that are running the BlackBerry® Application Suite can use all the IT policy rules that are associated with the supported features of the BlackBerry Application Suite. The BlackBerry Application Suite ignores IT policy rules that are associated with unsupported features.

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

To support new BlackBerry® Device Software versions, you can add new IT policy rules to a BlackBerry® Enterprise Server version that is earlier than the minimum requirement for those IT policy rules. For more information, visit [www.blackberry.com/btsc](http://www.blackberry.com/btsc) to read article KB-05439 How To - Import IT policy rules for BlackBerry Device Software 4.2

# Descriptions of IT policy rules

2

## 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.

**Default value**

The default value is False.

**Usage**

Change this rule to True to prevent a BlackBerry device user from accessing the application center.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.7
- BlackBerry® Enterprise Server version 4.1 SP6

### Disable Carrier Directory IT policy rule

**Description**

This rule specifies whether to prevent a user from accessing the carrier directory in the application center on a BlackBerry® device.

**Default value**

The default value is False.

**Usage**

Change this rule to True to prevent a user from accessing the carrier directory in the application center.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.7
- BlackBerry® Enterprise Server version 4.1 SP6

## BlackBerry Messenger policy group

### Disable BlackBerry Messenger IT policy rule

#### Description

This rule specifies whether BlackBerry® Messenger is turned off.

#### Default value

The default value is False.

#### Usage

Change this rule to True to turn off BlackBerry Messenger. This might help prevent risks that are associated with PIN messaging. For more information about PIN messaging risks, see the *BlackBerry Enterprise Solution Security Technical Overview*.

#### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 3.6
- BlackBerry® Enterprise Server version 4.0 SP2

### 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.

#### Default value

The default value is False.

#### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.6
- BlackBerry® Enterprise Server version 4.1 SP6

### Messenger Audit Email Address IT policy rule

#### Description

This rule specifies the address that the BlackBerry® device sends BlackBerry® Messenger audit reports to.

#### Default value

The default value is a null value. BlackBerry Messenger turns off auditing and does not send reports.

### Usage

Configure a value for this rule if you want to audit the use of BlackBerry Messenger in your organization.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 3.6
- BlackBerry® Enterprise Server version 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 that are sent by a BlackBerry device when there is no new data. The permitted range is 1 through 8736 hours.

### Default value

The default value is 168 hours.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 3.6
- BlackBerry® Enterprise Server version 4.0 SP2

## Messenger Audit Report Interval IT policy rule

### Description

This rule specifies the amount of time (in hours) that can elapse between BlackBerry® Messenger audit reports that are sent by a BlackBerry device when there is new data. The permitted range is 1 through 8736 hours.

### Default value

The default value is 24 hours.

### Usage

Change this rule to a shorter interval to manage the BlackBerry device memory.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 3.6

- BlackBerry® Enterprise Server version 4.0 SP2

## Messenger Audit UID IT policy rule

### Description

This rule specifies the unique identifier of the service book to use when a BlackBerry® device sends BlackBerry® Messenger audit reports.

### Default value

The default value is a null value. The BlackBerry device uses the first available service that encrypts messages to send reports.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 3.6
- BlackBerry® Enterprise Server version 4.0 SP2

## 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 previously connected computer or BlackBerry® device can reconnect to a BlackBerry® Smart Card Reader automatically.

Turning off automatic reconnections is designed to increase the life of the BlackBerry device battery.

### Default value

The default value is a null value.

### Usage

Select the Disable Auto Reconnect On BlackBerry option to prevent a BlackBerry device from reconnecting automatically to a BlackBerry Smart Card Reader.

Select the Disable Auto Reconnect On PC option to prevent a computer from reconnecting automatically to a BlackBerry Smart Card Reader.

### Minimum requirements

- Java® based BlackBerry device

- BlackBerry® Device Software version 4.0
- BlackBerry® Enterprise Server version 4.0 SP7
- BlackBerry Smart Card Reader software version 1.5.1

## Force Erase All Keys on BlackBerry Disconnected Timeout IT policy rule

### Description

This rule specifies whether the secure pairing keys for connections between a computer or a BlackBerry® device and the BlackBerry® Smart Card Reader are deleted after the connection closes.

### Default value

The default value is False. The secure pairing keys are not deleted from the BlackBerry device or the computer.

### Usage

If you change this rule to True, a user cannot change this feature on a BlackBerry device.

### Dependencies

A BlackBerry device uses this rule only if you configure the Maximum BlackBerry Disconnect Timeout IT policy rule.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.0
- BlackBerry® Enterprise Server version 4.0 SP5
- BlackBerry Smart Card Reader software version 1.5

## Force Erase Key on PC Standby IT policy rule

### Description

This rule specifies whether the computer deletes the secure pairing key and closes the connection to the BlackBerry® Smart Card Reader when the computer goes into standby mode.

### Default value

The default value is False.

### Usage

The user can configure this feature on the computer. If you change this rule to True, the user cannot turn off this feature on the computer.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.0
- BlackBerry® Enterprise Server version 4.0 SP7

- BlackBerry Smart Card Reader software version 1.5.1

## Maximum BlackBerry Disconnected Timeout IT policy rule

### Description

This rule specifies the maximum time (in seconds) of inactivity after the Bluetooth® connection between a BlackBerry® device and a BlackBerry® Smart Card Reader closes that the disconnected timeout expires. The permitted range is 0 through 604,800 seconds.

### Default value

The default value is a null value. The secure pairing information is not deleted from the BlackBerry device.

### Usage

If you configure this rule, the user cannot turn off this feature, but can change the Disconnected Timeout field on a BlackBerry device to a lower value.

If you do not configure this rule, the user can change the Disconnected Timeout value to any value.

### Dependencies

The value of this rule affects how a BlackBerry device uses the Force Erase All Keys on BlackBerry Disconnected Timeout IT policy rule, if you configure that rule to True.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.0
- BlackBerry® Enterprise Server version 4.0 SP2
- BlackBerry Smart Card Reader software version 1.5

### Exceptions

The BlackBerry® Enterprise Server for Novell® GroupWise® does not support this rule.

## Maximum BlackBerry Bluetooth Traffic Inactivity Timeout IT policy rule

### Description

This rule specifies the maximum time (in minutes) of inactivity that is permitted between a BlackBerry® Smart Card Reader and a BlackBerry device before the secure pairing information is deleted from the BlackBerry device and the BlackBerry Smart Card Reader. The permitted range is 1 through 10,080 minutes.

Activity is any secure packet that is sent or received by a BlackBerry device and a BlackBerry Smart Card Reader over a Bluetooth® connection, other than the connection heartbeat packet.

### Default value

The default value is a null value. The secure pairing information is not deleted from the BlackBerry device.

### Usage

If you configure this rule, the user cannot turn off this feature, but can change the Inactivity Timeout field on the BlackBerry device to a lower value.

If you do not configure this rule, the user can change the Inactivity Timeout field to any value.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.0
- BlackBerry® Enterprise Server version 4.0 SP2
- BlackBerry Smart Card Reader software version 1.5.1

### Exceptions

The BlackBerry® Enterprise Server for Novell® GroupWise® does not support this rule.

## Maximum BlackBerry Long Term Timeout IT policy rule

### Description

This rule specifies the maximum time (in hours) that can elapse after a BlackBerry® device and a BlackBerry® Smart Card Reader establish secure pairing information before the BlackBerry device and the BlackBerry Smart Card Reader delete the secure pairing information. The permitted range is 1 through 720 hours.

### Default value

The default value is a null value.

### Usage

If you configure this rule, the user cannot turn off this feature, but can change the Long Term Timeout field on a BlackBerry device to a lower value.

If you do not configure this rule, the user can change the Long Term Timeout field to any value.

### Dependencies

This rule is related to the Maximum BlackBerry Bluetooth Traffic Inactivity Timeout IT policy rule.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.0
- BlackBerry® Enterprise Server version 4.0 SP2
- BlackBerry Smart Card Reader software version 1.5.1

### Exceptions

The BlackBerry® Enterprise Server for Novell® GroupWise® does not support this rule.

## Maximum Bluetooth Encryption Key Regeneration Period IT policy rule

### Description

This rule specifies the length of time (in hours) that can elapse after a BlackBerry® Smart Card Reader regenerates a Bluetooth® encryption key if a BlackBerry device or computer is connected to a BlackBerry Smart Card Reader. If the BlackBerry device or computer is not connected to the BlackBerry Smart Card Reader, the BlackBerry Smart Card Reader regenerates the encryption key when the BlackBerry device or computer reconnects to the BlackBerry Smart Card Reader. The permitted range is 1 through 720 hours.

### Default value

The default value is a null value.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.0
- BlackBerry® Enterprise Server version 4.0 SP7
- BlackBerry Smart Card Reader software version 1.5.1

## 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%.

### Default value

The default value is 100%.

### Usage

Configure a larger power range for a BlackBerry device or a computer to communicate with a BlackBerry Smart Card Reader over a greater distance.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.0
- BlackBerry® Enterprise Server version 4.0 SP3
- BlackBerry Smart Card Reader software version 1.0

### Exceptions

The BlackBerry® Enterprise Server for Novell® GroupWise® does not support this rule.

## Maximum Connection Heartbeat Period IT policy rule

### Description

This rule specifies the maximum connection heartbeat period (in seconds). During each heartbeat period, a paired BlackBerry® device or computer sends a heartbeat which the BlackBerry® Smart Card Reader acknowledges. If either side fails to send or acknowledge a heartbeat in the maximum heartbeat period, the BlackBerry device or computer closes the Bluetooth® connection. The permitted range is 60 through 3600 seconds.

**Note:** If the disconnected timer is turned on, it starts when the connection closes. A BlackBerry device or computer deletes the secure pairing keys when the disconnected timeout expires.

### Default value

The default value is a null value. The heartbeat period is turned off.

### Usage

Use this rule to prevent an attacker from using a low-level Bluetooth heartbeat period to keep a Bluetooth connection between a BlackBerry device or computer and a BlackBerry Smart Card Reader open and the secure pairing keys present.

If you configure this rule, the user cannot turn off the heartbeat period but can change the Connection Heartbeat Period field on a BlackBerry device or a computer to a lower value.

If you do not configure this rule, the user can change the Connection Heartbeat Period field to any value.

If you configure a low value, such as 1, 2, or 5 minutes, Bluetooth traffic increases. The increased traffic might affect the battery power level of the BlackBerry device and BlackBerry Smart Card Reader.

### Dependencies

You can use the Maximum BlackBerry Disconnected Timeout and Maximum PC Disconnected Timeout IT policy rules to specify the BlackBerry device and the computer disconnected timers.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.0
- BlackBerry® Enterprise Server version 4.0 SP2
- BlackBerry Smart Card Reader software version 1.0

### Exceptions

The BlackBerry® Enterprise Server for Novell® GroupWise® does not support this rule.

## Maximum Number of BlackBerry Transactions IT policy rule

### Description

This rule specifies the maximum number of smart card-related transactions that can occur between a BlackBerry® device and a BlackBerry® Smart Card Reader before the secure pairing information is deleted from the BlackBerry device. The permitted range is 100 through 10,000 transactions.

A transaction is any set of request and response packets other than the connection heartbeat packet.

**Default value**

The default value is a null value. The secure pairing information is not deleted from the BlackBerry device.

**Usage**

If you configure this rule, the user cannot stop the secure pairing information from being deleted, but can change the Number of Transactions field on a BlackBerry device to a lower value.

If you do not configure this rule, the user can change the Number of Transactions field to any value.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.0
- BlackBerry® Enterprise Server version 4.0 SP2
- BlackBerry Smart Card Reader software version 1.5

**Exceptions**

The BlackBerry® Enterprise Server for Novell® GroupWise® does not support this rule.

## Maximum Number of PC Pairings IT policy rule

**Description**

This rule specifies the maximum number of computers that can pair with a BlackBerry® Smart Card Reader. The permitted range is 0 through 65,535 computers.

**Default value**

The default value is a null value.

**Usage**

If you configure this rule while computers are paired with 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 pair.

**Minimum requirements**

- BlackBerry® Enterprise Server version 4.0 SP5
- BlackBerry Smart Card Reader software version 1.5

**Exceptions**

The BlackBerry® Enterprise Server for Novell® GroupWise® does not support this rule.

## Maximum PC Bluetooth Traffic Inactivity Timeout IT policy rule

### Description

This rule specifies the maximum time (in minutes) of inactivity that is permitted between a BlackBerry® Smart Card Reader and a computer before the secure pairing information is deleted from the computer and the BlackBerry Smart Card Reader. The permitted range is 1 through 10,080 minutes.

Activity is any secure packet that is sent or received by a BlackBerry device and a BlackBerry Smart Card Reader over a Bluetooth® connection, other than the connection heartbeat packet.

### Default value

The default value is a null value. The secure pairing information is not deleted from the computer.

### Usage

If you configure this rule, the user cannot turn off this feature, but can change the Inactivity Timeout field in the BlackBerry Smart Card Reader options on the computer to a lower value.

If you do not configure this rule, the user can change the Inactivity Timeout field to any value.

### Minimum requirements

- BlackBerry® Enterprise Server version 4.0 SP5
- BlackBerry Smart Card Reader software version 1.5

### Exceptions

The BlackBerry® Enterprise Server for Novell® GroupWise® does not support this rule.

## Maximum Number of PC Transactions IT policy rule

### Description

This rule specifies the maximum number of smart card-related transactions that can occur between a computer and a BlackBerry® Smart Card Reader before the secure pairing information is deleted from the computer and the BlackBerry Smart Card Reader. The permitted range is 100 through 10,000 transactions.

A transaction is any set of request and response packets other than the connection heartbeat packet.

### Default value

The default value is a null value.

### Usage

If you configure this rule, the user cannot stop the secure pairing information from being deleted, but 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.

**Minimum requirements**

- BlackBerry® Enterprise Server version 4.0 SP5
- BlackBerry Smart Card Reader software version 1.5

**Exceptions**

The BlackBerry® Enterprise Server for Novell® GroupWise® does not support this rule.

## Maximum PC Disconnected Timeout IT policy rule

**Description**

This rule specifies the maximum time (in seconds) that can elapse after a computer and a BlackBerry® Smart Card Reader close a Bluetooth® connection before the secure pairing information for that connection is deleted from the computer and BlackBerry Smart Card Reader. The permitted range is 0 through 604,800 seconds.

**Default value**

The default value is a null value.

**Usage**

If you configure this rule, the user cannot turn off this feature, but can change the Disconnected Timeout 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 Disconnected Timeout field to any value.

**Minimum requirements**

- BlackBerry® Enterprise Server version 4.0 SP5
- BlackBerry Smart Card Reader software version 1.5

**Exceptions**

The BlackBerry® Enterprise Server for Novell® GroupWise® does not support this rule.

## Maximum PC Long Term Timeout IT policy rule

**Description**

This rule specifies the maximum time (in hours) that can elapse after a computer and a BlackBerry® Smart Card Reader establish secure pairing information before the computer and BlackBerry Smart Card Reader delete the secure pairing information. The permitted range is 1 through 720 hours.

**Default value**

The default value is a null value.

**Usage**

If you configure this rule, the user cannot turn off this feature, but can change the Long Term Timeout 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 Long Term Timeout field to any value.

### **Dependencies**

This rule is related to the Maximum PC Bluetooth Traffic Inactivity Timeout IT policy rule.

### **Minimum requirements**

- BlackBerry® Enterprise Server version 4.0 SP5
- BlackBerry Smart Card Reader software version 1.5

### **Exceptions**

The BlackBerry® Enterprise Server for Novell® GroupWise® does not support this rule.

## **Maximum Smart Card Not Present Timeout IT policy rule**

### **Description**

This rule specifies the maximum time (in seconds) that can elapse after a user removes a smart card from a BlackBerry® Smart Card Reader before the secure pairing information is deleted from the BlackBerry device and BlackBerry Smart Card Reader. The permitted range is 0 through 86,400 seconds.

### **Default value**

The default value is a null value. The secure pairing information is not deleted from the BlackBerry device.

### **Usage**

If you configure this rule, the user can change the Card Not Present Timeout value on the BlackBerry device to any value.

If you do not configure this rule, the user cannot turn off this feature, but can change the Card Not Present Timeout field to a lower value.

### **Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.0
- BlackBerry® Enterprise Server version 4.0 SP2
- BlackBerry Smart Card Reader software version 1.5

### **Exceptions**

The BlackBerry® Enterprise Server for Novell® GroupWise® does not support this rule.

## 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.

#### Default value

The default value is False.

#### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.2.2
- BlackBerry® Enterprise Server version 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.

#### Default value

The default value is False.

#### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.2.2
- BlackBerry® Enterprise Server version 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 the user can place outgoing calls from a BlackBerry® device using Bluetooth® technology.

**Default value**

The default value is Always.

**Usage**

Configure this rule to Always, Never, or Only when the BlackBerry device is unlocked.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.0.2
- BlackBerry® Enterprise Server version 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® enabled device.

**Default values**

The default value in the Advanced security and Advanced security (disallow application downloads) IT policies is True.

The default value in all other preconfigured IT policies is False.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.1
- BlackBerry® Enterprise Server version 4.0 SP3

## Disable Advanced Audio Distribution Profile IT policy rule

**Description**

This rule specifies whether a Bluetooth® enabled BlackBerry® device can use the Bluetooth A2DP.

**Default value**

The default value is False.

**Usage**

Change this rule to True to turn off the ability to stream audio using Bluetooth technology.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.2.2

- BlackBerry® Enterprise Server version 4.1 SP4

## Disable Audio/Video Remote Control Profile IT policy rule

### Description

This rule specifies whether a Bluetooth® enabled BlackBerry® device can use the Bluetooth AVRCP.

### Default value

The default value is False.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.2.2
- BlackBerry® Enterprise Server version 4.1 SP4

## Disable Bluetooth IT policy rule

### Description

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

### Default value

The default value is False.

### Usage

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

### Minimum requirement

- Java® based BlackBerry device
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 3.8
- BlackBerry® Enterprise Server version 4.0

### Exceptions

The BlackBerry® Enterprise Server for Novell® GroupWise® supports this rule in BlackBerry Device Software version 4.0 and later.

## 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.

**Default value**

The default value is True.

**Minimum requirements**

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

**Default value**

The default value is False.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.2
- BlackBerry® Enterprise Server version 4.0 SP6

## Disable Discoverable Mode IT policy rule

**Description**

This rule specifies whether to prevent BlackBerry® device users from making their BlackBerry device discoverable.

A BlackBerry device that is discoverable can be found by other Bluetooth® enabled devices within range of the BlackBerry device.

**Default values**

The default value in the Default and Basic password security IT policies is False.

The default value in all other preconfigured IT policies is True.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.0.2
- BlackBerry® Enterprise Server version 4.0 SP2

## Disable File Transfer IT policy rule

### Description

This rule specifies whether to prevent a BlackBerry® device from exchanging files with supported Bluetooth® OBEX devices.

### Default values

The default value in the Advanced security and Advanced security (disallow application downloads) IT policies is True.

The default value in all other preconfigured IT policies is False.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.2
- BlackBerry® Enterprise Server version 4.0 SP6

## Disable Handsfree Profile IT policy rule

### Description

This rule specifies whether a BlackBerry® device can use the Bluetooth® HFP.

### Default value

The default value is False.

### Usage

A BlackBerry device uses the Bluetooth HFP to connect to most car kits and some headsets.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 3.8
- BlackBerry® Enterprise Server version 4.0

### Exceptions

The BlackBerry® Enterprise Server for Novell® GroupWise® supports this rule in BlackBerry Device Software versions 4.0 and later.

## Disable Headset Profile IT policy rule

### Description

This rule specifies whether a BlackBerry® device can use the Bluetooth® HSP.

### Default value

The default value is False.

### Usage

A BlackBerry device uses the Bluetooth HSP to connect to most headsets and some car kits.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 3.8
- BlackBerry® Enterprise Server version 4.0

### Exceptions

The BlackBerry® Enterprise Server for Novell® GroupWise® supports this rule in BlackBerry Device Software versions 4.0 and later.

## Disable Pairing IT policy rule

### Description

This rule specifies whether a BlackBerry® device can pair with a Bluetooth® enabled device.

### Default value

The default value is False.

### Usage

After a BlackBerry device pairs with a supported Bluetooth enabled device, you can use this rule to prevent the BlackBerry device from pairing with other Bluetooth enabled devices.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 3.8
- BlackBerry® Enterprise Server version 4.0

### Exceptions

The BlackBerry® Enterprise Server for Novell® GroupWise® supports this rule in BlackBerry Device Software version 4.0 and later.

## Disable Serial Port Profile IT policy rule

### Description

This rule specifies whether a BlackBerry® device can use the Bluetooth® SPP.

### Default values

The default value in the Advanced security and Advanced security (disallow application downloads) IT policies is True.

The default value in all other preconfigured IT policies is False.

### Usage

A BlackBerry device uses the Bluetooth SPP to establish a serial connection between the BlackBerry device and a Bluetooth enabled device that uses a serial port interface.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 3.8
- BlackBerry® Enterprise Server version 4.0

### Exceptions

The BlackBerry® Enterprise Server for Novell® GroupWise® supports this rule in BlackBerry Device Software version 4.0 and later.

## Disable SIM Access Profile IT policy rule

### Description

This rule specifies whether to prevent a Bluetooth® enabled BlackBerry® device from using the Bluetooth SIM Access Profile, which might be required when a car kit initiates dialing.

### Default value

The default value is False.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.6
- BlackBerry® Enterprise Server version 4.1 SP6

## Disable Wireless Bypass IT policy rule

### Description

This rule specifies whether a BlackBerry® device uses wireless bypass using Bluetooth® technology.

### Default value

The default value is True.

### Minimum requirements

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

### Default value

The default value is False.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Desktop Software version 4.2.2
- BlackBerry® Device Software version 4.2.2
- BlackBerry® Enterprise Server version 4.1 SP4

## Limit Discoverable Time IT policy rule

### Description

This rule specifies whether a BlackBerry® device user can configure the Bluetooth® discoverable mode option so that it does not have a time limit.

### Default value

The default value is False.

### Usage

Change this rule to True to permit a user to set the Bluetooth discoverable mode option to use a time limit of 2 minutes or to turn off Bluetooth discoverable mode.

### Dependencies

A BlackBerry device uses this rule only if you configure the Disable Discoverable Mode IT policy rule to False.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.5
- BlackBerry® Enterprise Server version 4.1 SP5

## Minimum Encryption Key Length IT policy rule

### Description

This rule specifies the minimum encryption key length (in bytes) that a BlackBerry® device uses to encrypt Bluetooth® connections. The permitted range is 1 through 16 bytes.

**Default value**

The default value is 1 byte.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.5
- BlackBerry® Enterprise Server version 4.1 SP5

## Require Encryption IT policy rule

**Description**

This rule specifies whether a BlackBerry® device uses Bluetooth® encryption for all connections.

**Default value**

The default value is False.

**Usage**

If you change this rule to True to require Bluetooth encryption for all connections, you might restrict compatibility with some Bluetooth enabled devices.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.1
- BlackBerry® Enterprise Server version 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® enabled device.

**Default values**

The default value in the Advanced security and Advanced security (disallow application downloads) IT policies is True.

The default value in all other preconfigured IT policies is False.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.2
- BlackBerry® Enterprise Server version 4.0 SP6

## Require Password for Discoverable Mode IT policy rule

### Description

This rule specifies whether a user must type the BlackBerry® device password before a BlackBerry device can be discovered by Bluetooth® enabled devices.

### Default value

The default value is False.

### Dependencies

A BlackBerry device uses this rule only if the Password Required IT policy rule is configured to True.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.1
- BlackBerry® Enterprise Server version 4.0 SP3

## Require Password for Enabling Bluetooth Support IT policy rule

### Description

This rule specifies whether a user must type the BlackBerry® device password to turn on Bluetooth® technology.

### Default value

The default value is False.

### Dependencies

A BlackBerry device uses this rule only if the Password Required IT policy rule is configured to True.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.1
- BlackBerry® Enterprise Server version 4.0 SP3

## Browser policy group

IT policy 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 application download service icons appear on a BlackBerry® device when the wireless service provider assigns a service to a BlackBerry device and the appropriate service books are present on the BlackBerry device.

**Default value**

The default value is True.

**Usage**

Change this rule to False to hide all application download service icons.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.3
- BlackBerry® Enterprise Server version 4.1 SP5

## Allow Hotspot Browser IT policy rule

**Description**

This rule specifies whether a Wi-Fi® enabled BlackBerry® device can access a hotspot browser.

**Default value**

The default value is Allow.

**Usage**

Change this rule to Disallow to prevent a Wi-Fi enabled BlackBerry device from accessing a hotspot browser.

Change this rule to Only for Hotspot Login to permit access only for the purpose of authenticating to the hotspot.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.6
- BlackBerry® Enterprise Server version 4.1 SP6

## Allow IBS Browser IT policy rule

**Description**

This rule specifies whether a separate icon appears on a BlackBerry® device if the appropriate service books are present for BlackBerry Internet Service Browsing.

**Default value**

The default value is True.

**Usage**

Change this rule to False to hide the separate browser icon.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0 (internal)
- BlackBerry® Device Software version 4.0
- BlackBerry® Enterprise Server version 4.0 SP1

## Disable Auto Synchronization in Browser IT policy rule

**Description**

This rule specifies whether to prevent a user from configuring intervals for auto synchronization of the bookmark list in the BlackBerry® Browser.

**Default value**

The default value is False.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 4.2
- BlackBerry® Enterprise Server version 4.0 SP6

## Disable JavaScript in Browser IT policy rule

**Description**

This rule specifies whether the BlackBerry® Browser can run JavaScript®.

**Default value**

The default value is False.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0 (internal)
- BlackBerry® Device Software version 4.0
- BlackBerry® Enterprise Server version 4.0

## Download Images URL IT policy rule

### Description

This rule specifies a web address that provides additional pictures for a BlackBerry® device.

### Default value

The default value is a null value.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0 SP3
- BlackBerry® Device Software version 4.1

## Download Themes URL IT policy rule

### Description

This rule specifies a web address that provides additional themes for a BlackBerry® device.

### Default value

The default value is a null value.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 4.1
- BlackBerry® Enterprise Server version 4.0 SP3

## Download Tunes URL IT policy rule

### Description

This rule specifies a web address that provides additional ring tones for a BlackBerry® device.

### Default value

The default value is a null value.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 4.1

- BlackBerry® Enterprise Server version 4.0 SP3

## MDS Browser BSM Enabled IT policy rule

### Description

This rule specifies whether the browser session manager is turned on in the BlackBerry® Browser.

### Default value

The default value is True.

### Usage

The browser session manager is designed to improve BlackBerry Browser performance by helping the BlackBerry® MDS Connection Service use the BlackBerry Browser cache.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0 (internal)
- BlackBerry® Device Software version 4.0.2
- BlackBerry® Enterprise Server version 4.0 SP2

## MDS Browser Domains IT policy rule

### Description

This rule specifies a list of web addresses that a BlackBerry® device retrieves using the BlackBerry® Browser. Separate multiple web addresses with a comma.

### Default value

The default value is a null value.

### Usage

This rule supports the use of wildcard characters.

If you want to permit the BlackBerry Browser to retrieve sub-domains of a web address, prefix the domain with a period. For example, type ".yahoo.ca" to permit the BlackBerry Browser to retrieve all sub-domains of yahoo.ca (such as mail.yahoo.ca, www.yahoo.ca).

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 4.2
- BlackBerry® Enterprise Server version 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.

### Default value

The default value is False.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0 (internal)
- BlackBerry® Device Software version 4.0.2
- BlackBerry® Enterprise Server version 4.0 SP2

## MDS Browser JavaScript Enabled IT policy rule

### Description

This rule specifies whether JavaScript® in the BlackBerry® Browser is turned on.

### Default value

The default value is False.

### Usage

Change this rule to True to render web pages that use JavaScript correctly.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0 (internal)
- BlackBerry® Device Software version 4.0.2
- BlackBerry® Enterprise Server version 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.

### Default value

The default value is False.

#### **Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0 (internal)
- BlackBerry® Device Software version 4.0.2
- BlackBerry® Enterprise Server version 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**

The default value is BlackBerry Browser.

### **Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0 (internal)
- BlackBerry® Device Software version 3.6
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.6
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® and Novell® GroupWise® version 4.0

## **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.

### **Default value**

The default value is False.

### **Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 4.2
- BlackBerry® Enterprise Server version 4.0 SP6

## Camera policy group

### Disable Photo Camera IT policy rule

**Description**

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

**Default value**

The default value is False.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.2
- BlackBerry® Enterprise Server version 4.0 SP6

### Disable Video Camera IT policy rule

**Description**

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

**Default value**

The default value is False.

**Usage**

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

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.3
- BlackBerry® Enterprise Server version 4.1 SP5

## Certificate Synchronization policy group

IT policy 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 web site for a white noise machine). If the S/MIME Support Package for BlackBerry® Smartphones version 4.0 or later is installed on a BlackBerry device, the certificate synchronization tool of the BlackBerry® Desktop Manager can use the web address to retrieve random data to add to a BlackBerry device.

### Default value

The default value is a null value.

### Minimum requirements

- S/MIME Support Package for BlackBerry Smartphones version 4.0
- BlackBerry® Application Suite version 1.0
- BlackBerry® Desktop Software version 4.0
- BlackBerry® Enterprise Server version 4.0

### Exceptions

The BlackBerry® Enterprise Server for Novell® GroupWise® does not support this rule.

## User Can Disable Automatic RNG Initialization IT policy rule

### Description

This rule specifies whether a user can stop the BlackBerry® Desktop Software from starting the random number generator on a BlackBerry device automatically.

### Default setting

The default value is True.

### Minimum requirements

- BlackBerry Desktop Software version 4.3
- BlackBerry® Enterprise Server version 4.1 SP5

## Common policy group

### BlackBerry Server version IT policy rule

#### Description

This rule specifies the BlackBerry® Enterprise Server version number that the BlackBerry Enterprise Server sends to a BlackBerry device.

**Note:** Where applicable, if you do not configure this rule, a BlackBerry device uses the settings that the application control policy rules specify, or the software configurations that the BlackBerry device configuration tool define. If application control data does not exist, by default the BlackBerry device opens internal and external connections through the firewall.

### Default value

The default value is a null value.

### Usage

Configure this rule to 4.0 to support application control features.

This rule is obsolete in BlackBerry Enterprise Server version 4.1 and later.

### Minimum requirements

- C++ based BlackBerry device that is running BlackBerry Device Software version 2.7
- Java® based BlackBerry device that is running BlackBerry® Device Software version 4.0
- BlackBerry® Connect™ version 4.0
- BlackBerry Enterprise Server version 4.0 and preceding

## Confirm On Send IT policy rule

### Description

This rule specifies whether users must confirm before they send an email message, PIN message, SMS text message, or MMS message.

### Default value

The default value is a null value.

### Usage

Use this rule to create a customized confirmation message.

### Minimum requirements

- Java® based BlackBerry® device that is running BlackBerry® Device Software version 4.0
- C++-based BlackBerry device that is running BlackBerry Device Software version 2.7
- BlackBerry® Enterprise Server version 4.0
- BlackBerry® Connect™ version 4.0
- BlackBerry® Application Suite version 1.0

### Exceptions

The BlackBerry® Enterprise Server for Novell® GroupWise® supports this rule only for Java based BlackBerry devices.

## Disable Kodiak PTT IT policy rule

### Description

This rule specifies whether a BlackBerry® device user can use Kodiak™ PTT on a supported BlackBerry device.

### Default value

The default value is False.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.2
- BlackBerry® Enterprise Server version 4.0 SP6

## Disable MMS IT policy rule

### Description

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

### Default value

The default value is False.

### Usage

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

### Dependencies

To block incoming MMS messages, in the Security policy group, configure the Firewall Block Incoming Messages IT policy rule.

### Minimum requirements

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

## Disable Voice-Activated Dialing IT policy rule

### Description

This rule specifies whether voice dialing is available on a BlackBerry® device.

### Default value

The default value is False.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.2
- BlackBerry® Enterprise Server version 4.0 SP6

## Disable Voice Note Recording IT policy rule

**Description**

This rule specifies whether the voice note recording feature on a BlackBerry® device is turned on.

**Default value**

The default value is False.

**Usage**

Change this rule to True to turn off the voice note recording feature and to prevent applications on a BlackBerry device from accessing this feature.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.3
- BlackBerry® Enterprise Server version 4.1 SP5

## IT Policy Notification IT policy rule

**Description**

This rule specifies whether warnings about IT policy changes appear to a BlackBerry® device user.

**Default value**

The default value is False.

**Minimum requirements**

- C++-based BlackBerry device that is running BlackBerry® Device Software version 2.7
- Java® based BlackBerry device that is running BlackBerry Device Software version 4.0
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0
- BlackBerry® Enterprise Server version 4.0

**Exceptions**

The BlackBerry® Enterprise Server for Novell® GroupWise® supports this rule only for Java based BlackBerry devices.

## Lock Owner Info IT policy rule

### Description

This rule specifies whether a user can change the owner information for a BlackBerry® device. You can lock the Information field, the Name field, or both fields.

### Default value

The default value is a null value.

### Usage

Configure this rule to Lock Information text that is defined using the Set Owner Info IT Policy rule.

Configure this rule to Lock Name text that is defined using the Set Owner Name IT Policy rule.

Configure this rule to Lock both Name and Information text that is defined using the Set Owner Info and Set Owner Name IT policy rules.

You can overwrite this information by sending the Set Owner Information IT administration command to a BlackBerry device.

### Dependencies

The Lock Owner Info IT policy rule is related to the Set Owner Info and Set Owner Name IT Policy rules.

### Minimum requirements

- C++-based BlackBerry device that is running BlackBerry® Device Software version 2.7
- Java® based BlackBerry device that is running BlackBerry Device Software version 4.0
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0
- BlackBerry® Enterprise Server version 4.0

### Exceptions

The BlackBerry® Enterprise Server for Novell® GroupWise® supports this rule only for Java based BlackBerry devices.

## Set Owner Info IT policy rule

### Description

This rule specifies the owner information that appears on a BlackBerry® device.

### Default value

The default value is a null value.

### Usage

You can overwrite this information by sending the Set Owner Information IT administration command to a BlackBerry device.

### **Dependencies**

The Set Owner Info IT policy rule is related to the Lock Owner Info IT policy rule.

### **Minimum requirements**

- C++-based BlackBerry device that is running BlackBerry® Device Software version 2.7
- Java® based BlackBerry device that is running BlackBerry Device Software version 4.0
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0
- BlackBerry® Enterprise Server version 4.0

### **Exceptions**

The BlackBerry® Enterprise Server for Novell® GroupWise® supports this rule only for Java based BlackBerry devices.

## **Set Owner Name IT policy rule**

### **Description**

This rule specifies the owner name that appears on a BlackBerry® device.

### **Default value**

The default value is a null value.

### **Usage**

You can overwrite this information by sending the Set Owner Information IT administration command to a BlackBerry device.

### **Dependencies**

The Set Owner Name IT policy rule is related to the Lock Owner Info IT policy rule.

### **Minimum requirements**

- C++-based BlackBerry device that is running BlackBerry® Device Software version 2.7
- Java® based BlackBerry device that is running BlackBerry Device Software version 4.0
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0
- BlackBerry® Enterprise Server version 4.0

### **Exceptions**

The BlackBerry® Enterprise Server for Novell® GroupWise® supports this rule only for Java based BlackBerry devices.

## Desktop Only items

### 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 Manager or BlackBerry® Web Desktop Manager is turned on.

#### Default value

The default value is False.

#### Usage

To permit the backup and restore tool to back up BlackBerry device data automatically, change this rule to True. Automatic backups can help provide recent BlackBerry device data for recovery if you need to replace a lost or stolen BlackBerry device.

#### Minimum requirements

- BlackBerry® Application Suite version 1.0
- BlackBerry® Desktop Software version 3.5 or BlackBerry® Web Desktop Manager version 1.0
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® and Novell® GroupWise® version 4.0
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.5

#### Exceptions

The BlackBerry Enterprise Server for Novell GroupWise supports this rule with the BlackBerry Web Desktop Manager only.

### Auto Backup Exclude Messages IT policy rule

#### Description

This rule specifies whether messages are excluded when an automatic backup occurs.

#### Default value

The default value is False.

#### Dependencies

If you change this rule to True, you must configure the Auto Backup Include All IT policy rule to False.

The BlackBerry® Enterprise Server for Novell® GroupWise® supports this rule with the BlackBerry® Web Desktop Manager only.

#### Minimum requirements

- BlackBerry® Application Suite version 1.0
- BlackBerry® Desktop Software version 3.5 or BlackBerry Web Desktop Manager version 1.0

- BlackBerry® Enterprise Server for IBM® Lotus® Domino® and BlackBerry® Enterprise Server for Novell® GroupWise® version 4.0
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.5

**Exceptions**

The BlackBerry Enterprise Server for Novell GroupWise supports this rule with the BlackBerry Web Desktop Manager only.

## Auto Backup Exclude Sync IT policy rule

**Description**

This rule specifies whether application data that is synchronized with desktop organizer applications is excluded when an automatic backup occurs.

**Default value**

The default value is False.

**Dependencies**

If you change this rule to True, you must configure the Auto Backup Include All IT policy rule to False.

**Minimum requirements**

- BlackBerry® Application Suite version 1.0
- BlackBerry® Desktop Software version 3.5 or BlackBerry Web Desktop Manager version 1.0
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® and BlackBerry® Enterprise Server for Novell® GroupWise® version 4.0
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.5

**Exceptions**

The BlackBerry Enterprise Server for Novell GroupWise supports this rule with the BlackBerry Web Desktop Manager only.

## Auto Backup Frequency IT policy rule

**Description**

This rule specifies how often (in days) automatic backups occur. The permitted range is 1 through 99 days.

**Default value**

The default value is 7 days.

**Usage**

Change this value to a minimum of 2 days so that backups of BlackBerry® device data occur more frequently, to a maximum of 99 days.

If a user's computer memory is limited, save backup files to a network drive.

**Minimum requirements**

- BlackBerry® Application Suite version 1.0
- BlackBerry® Desktop Software version 3.5 or BlackBerry® Web Desktop Manager version 1.0
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® and Novell® GroupWise® version 4.0
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.5

**Exceptions**

The BlackBerry Enterprise Server for Novell GroupWise supports this rule with the BlackBerry Web Desktop Manager only.

## Auto Backup Include All IT policy rule

**Description**

This rule specifies whether all BlackBerry® device data is included when an automatic backup occurs.

**Default value**

The default value is True.

**Usage**

If you configure this rule to True, in the backup and restore tool options, the Backup all device application data option is selected.

If you configure the Auto Backup Exclude Sync or Auto Backup Exclude Messages IT policy rules to True, change this rule to False.

**Minimum requirements**

- BlackBerry® Application Suite version 1.0
- BlackBerry® Desktop Software version 3.5 or BlackBerry® Web Desktop Manager version 1.0
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® and Novell® GroupWise® version 4.0
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.5

**Exceptions**

The BlackBerry Enterprise Server for Novell GroupWise supports this rule with the BlackBerry Web Desktop Manager only.

## Disable Wireless Calendar IT policy rule

**Description**

This rule specifies whether users can use the wireless calendar synchronization option in the synchronize tool of the BlackBerry® Desktop Manager.

**Default value**

The default value is False.

**Usage**

Change this rule to True to prevent users from using wireless calendar synchronization.

**Minimum requirements**

- BlackBerry® Application Suite version 1.0
- BlackBerry® Desktop Software version 3.5 or BlackBerry® Web Desktop Manager version 1.0
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® and BlackBerry® Enterprise Server for Novell® GroupWise® version 4.0
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.5

**Exceptions**

The BlackBerry Enterprise Server for Novell GroupWise supports this rule with the BlackBerry Web Desktop Manager only.

## 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 user sends in the sent messages folder on the user's computer.

**Default value**

The default value is False.

**Usage**

Change this rule to True to store email messages that a user sends from a BlackBerry device.

**Minimum requirements**

- BlackBerry® Application Suite version 1.0
- BlackBerry® Desktop Software version 3.5 or BlackBerry® Web Desktop Manager version 1.0
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® and BlackBerry® Enterprise Server for Novell® GroupWise® version 4.0
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.5

**Exceptions**

The BlackBerry Enterprise Server for Novell GroupWise supports this rule with the BlackBerry Web Desktop Manager only.

## Force Load Count IT policy rule

**Description**

This rule specifies the number of times that users can decline to update the BlackBerry® Device Software before they must update it. The permitted range is -1 through 1000 times.

**Default value**

The default value is a null value.

### Usage

To turn off mandatory updates of the BlackBerry Device Software, configure this rule to -1.

To turn on the forced update feature, configure this rule to 0 or to a greater value. If you turn on the feature, when a user logs in and connects a BlackBerry device to a computer, the BlackBerry® Desktop Manager or BlackBerry® Web Desktop Manager version 1.0 or version 1.0.1 checks whether newer versions of the software are available automatically, and prompts the user to update the BlackBerry device.

### Minimum requirements

- BlackBerry® Application Suite version 1.0
- BlackBerry® Desktop Software version 3.5 or BlackBerry Web Desktop Manager version 1.0
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® and BlackBerry® Enterprise Server for Novell® GroupWise® version 4.0
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.5

### Exceptions

The BlackBerry Enterprise Server for Novell GroupWise supports this rule with the BlackBerry Web Desktop Manager only.

## Force Load Message IT policy rule

### Description

This rule specifies the message that appears when users are prompted to update the BlackBerry® Device Software to a later version.

### Default value

The default value is a null value.

### Dependencies

A BlackBerry device uses this rule only if you configure the Force Load Count IT policy rule to 0 or higher.

### Minimum requirements

- BlackBerry® Application Suite version 1.0
- BlackBerry® Desktop Software version 3.5 or BlackBerry® Web Desktop Manager version 1.0
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® and BlackBerry® Enterprise Server for Novell® GroupWise® version 4.0
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.5

### Exceptions

The BlackBerry Enterprise Server for Novell GroupWise supports this rule with the BlackBerry Web Desktop Manager only.

## 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.

The BlackBerry® Enterprise Server configures this value.

### Default value

The default value is True. By default, a BlackBerry device receives email messages from the inbox only.

### Usage

When you change this rule, the option changes in the email settings tool of the BlackBerry® Desktop Manager.

### Minimum requirements

- BlackBerry® Application Suite version 1.0
- BlackBerry® Desktop Software version 3.5
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® version 4.0
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.5

### Exceptions

The BlackBerry® Enterprise Server for Novell® GroupWise® does not support this rule.

## 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.

### Default value

The default value is True.

### Minimum requirements

- BlackBerry® Application Suite version 1.0
- BlackBerry® Desktop Software version 3.5
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® version 4.0
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.5

### Exceptions

The BlackBerry® Enterprise Server for Novell® GroupWise® does not support this rule.

## Message Prompt IT policy rule

### Description

This rule specifies the message that should appear when the BlackBerry® Desktop Software starts.

### Default value

The default value is a null value.

### Usage

You can use this rule when you manage BlackBerry devices that are running

### Minimum requirements

- BlackBerry® Application Suite version 1.0
- BlackBerry Desktop Software version 3.5
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® version 4.0
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.5

### Exceptions

The BlackBerry® Enterprise Server for Novell® GroupWise® does not support this rule.

## Show Application Loader IT policy rule

### Description

This rule specifies whether the application loader tool appears in BlackBerry® Desktop Manager and BlackBerry® Web Desktop Manager.

### Default value

The default value is True.

### Usage

Change this rule to False to hide the Device Software tab in BlackBerry Web Desktop Manager and the Application Loader icon in BlackBerry Desktop Manager.

### Minimum requirements

- BlackBerry® Application Suite version 1.0
- BlackBerry® Desktop Software version 3.5 or BlackBerry Web Desktop Manager version 1.0
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® version 4.0
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.5

### Exceptions

The BlackBerry® Enterprise Server for Novell® GroupWise® supports this rule with the BlackBerry Web Desktop Manager version 1.0 or version 1.0.1 only.

## Show Web Link IT policy rule

### Description

This rule specifies whether the link icon for the Internet appears in the BlackBerry® Desktop Manager.

### Default value

The default value is False.

### Usage

You can use this rule when you manage BlackBerry devices that are running BlackBerry® Application Suite versions 1.0 and later.

### Dependencies

The link icon appears only if you configure a default web address using the Web Link URL IT policy rule.

### Minimum requirements

- BlackBerry® Application Suite version 1.0
- BlackBerry® Desktop Software version 3.5
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® version 4.0
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.5

### Exceptions

The BlackBerry® Enterprise Server for Novell® GroupWise® does not support this rule.

## 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 user's computer and on the BlackBerry device instead of applying the changes to the BlackBerry device only.

### Default value

The default value is True.

### Minimum requirements

- BlackBerry® Application Suite version 1.0
- BlackBerry® Desktop Software version 3.5
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® version 4.0
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.5

### Exceptions

The BlackBerry® Enterprise Server for Novell® GroupWise® does not support this rule.

## Web Link Label IT policy rule

### Description

This rule specifies the name of the web link icon, if it appears in the BlackBerry® Desktop Manager.

### Default value

The default value is Downloads.

### Usage

Configure the label according to your organization's requirements.

### Dependencies

If you configure this rule, you must also configure the Show Web Link IT policy rule to True so that the web link icon appears.

### Minimum requirements

- BlackBerry® Application Suite version 1.0
- BlackBerry® Desktop Software version 3.5
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® version 4.0
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.5

### Exceptions

The BlackBerry® Enterprise Server for Novell® GroupWise® does not support this rule.

## 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 Manager.

### Default value

The default value is a null value.

### Dependencies

If you configure this rule, for the web link icon to appear, you must also configure the Show Web Link IT policy rule to True.

### Minimum requirements

- BlackBerry® Application Suite version 1.0
- BlackBerry® Desktop Software version 3.5
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® version 4.0

- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.5

**Exceptions**

The BlackBerry® Enterprise Server for Novell® GroupWise® does not support this rule.

## Desktop policy group

### Desktop Allow Desktop Add-ins IT policy rule

**Description**

This rule specifies whether the BlackBerry® Desktop Software can run add-in applications, such as third-party COM-based extensions that access BlackBerry device databases during synchronization.

**Default value**

The default value is True.

**Minimum requirements**

- BlackBerry® Application Suite version 1.0
- BlackBerry Desktop Software version 3.6
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® version 4.0
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.5

**Exceptions**

The BlackBerry® Enterprise Server for Novell® GroupWise® does not support this rule.

### 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.

**Default value**

The default value is True.

**Usage**

Change this rule to False to prevent users from switching to an unapproved BlackBerry device.

The Enterprise Service Policy overrides this rule. For more information about using the Enterprise Service Policy, see the *BlackBerry Enterprise Solution Security Technical Overview*.

**Minimum requirements**

- BlackBerry® Application Suite version 1.0
- BlackBerry Desktop Software version 3.5 or BlackBerry Web Desktop Manager version 1.0
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® and BlackBerry® Enterprise Server for Novell® GroupWise® version 4.0
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.5

**Exceptions**

The BlackBerry Enterprise Server for Novell GroupWise supports this rule with the BlackBerry Web Desktop Manager only.

## Desktop Password Cache Timeout IT policy rule

**Description**

This rule specifies the length of time (in minutes) that the BlackBerry® Desktop Software or BlackBerry® Web Desktop Manager caches the BlackBerry device password in memory. The permitted range is 0 through 720 minutes.

**Default value**

The default value is 10 minutes.

**Usage**

If you change this rule to 0, a BlackBerry device clears the password from memory when a user disconnects the BlackBerry device from a computer, regardless of the length of time that the BlackBerry device was connected.

**Dependencies**

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

**Minimum requirements**

- BlackBerry® Application Suite version 1.0
- BlackBerry Desktop Software version 3.5 or BlackBerry Web Desktop Manager version 1.0
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® and BlackBerry® Enterprise Server for Novell® GroupWise® version 4.0
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.5

**Exceptions**

The BlackBerry Enterprise Server for Novell GroupWise supports this rule with the BlackBerry Web Desktop Manager only.

## Disable Check For Updates Link IT policy rule

**Description**

This rule specifies whether the Check for updates link in the BlackBerry® Desktop Manager is available.

**Default value**

The default value is False.

**Minimum requirements**

- BlackBerry® Desktop Software version 4.5
- BlackBerry® Enterprise Server version 4.1 SP5

## Disable Media Manager IT policy rule

**Description**

This rule specifies whether the media manager tool of the BlackBerry® Desktop Manager is available.

**Default value**

The default value is False.

**Usage**

Change this rule to True to permit a user to access an external file system using the media manager tool.

**Minimum requirements**

- BlackBerry® Connect™ version 4.0 (internal)
- BlackBerry® Desktop Software version 4.2
- BlackBerry® Enterprise Server version 4.0 SP6

**Exceptions**

The BlackBerry® Enterprise Server for Novell® GroupWise® does not support this rule.

## 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 Manager.

**Minimum requirements**

- BlackBerry® Desktop Software version 4.5
- BlackBerry® Enterprise Server version 4.1 SP5

## Device IOT Application policy group

### Device Diagnostic App Disable IT policy rule

**Description**

This rule specifies whether to prevent a user from sending diagnostic reports from a BlackBerry® device.

**Default value**

The default value is False.

**Minimum requirements**

- BlackBerry® Application Suite version 1.0
- Java® based BlackBerry device
- BlackBerry® Device Software version 4.2
- BlackBerry® Enterprise Server version 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**

The default value is False.

**Minimum requirements**

- Java® based BlackBerry® device
- BlackBerry® Device Software version 4.2
- BlackBerry® Enterprise Server version 4.0 SP6
- BlackBerry® Application Suite version 1.0

## 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**

The default value is False.

**Minimum requirements**

- Java® based BlackBerry® device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 4.2
- BlackBerry® Enterprise Server version 4.0 SP6

## Device Only Items

### Allow BCC Recipients IT policy rule

#### Description

This rule specifies whether a user can include BCC recipients when they compose email messages on a BlackBerry® device.

#### Default value

The default value is True.

#### Minimum requirements

- C++-based BlackBerry device that is running BlackBerry® Device Software version 2.5
- Java® based BlackBerry device that is running BlackBerry Device Software version 3.6
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ versions 1.2, 2.0, 2.1, 4.0
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® and BlackBerry® Enterprise Server for Novell® GroupWise® version 4.0
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.5

#### Exceptions

The BlackBerry Enterprise Server for Novell GroupWise supports this rule only for Java based BlackBerry devices that are running BlackBerry Device Software version 4.0 and later.

### Allow Peer-to-Peer Messages IT policy rule

#### Description

This rule specifies whether a user can send PIN messages.

#### Default value

The default value is True.

#### Usage

Change this rule to False to prevent users from sending PIN messages.

Changing this rule to False does not prevent users from receiving PIN messages.

#### Dependencies

To block incoming PIN messages, in the Security policy group, configure the Firewall Block Incoming Messages IT policy rule to PIN Messages (Public) and PIN Messages (Corporate).

#### Minimum requirements

- C++-based BlackBerry device that is running BlackBerry® Device Software version 2.5
- Java® based BlackBerry device that is running BlackBerry Device Software version 3.6
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ versions 1.2, 2.0, 2.1, 4.0
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® and BlackBerry® Enterprise Server for Novell® GroupWise® version 4.0
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.5

### Exceptions

The BlackBerry Enterprise Server for Novell GroupWise supports this rule only for Java based BlackBerry devices that are running BlackBerry Device Software version 4.0 or later.

## Allow SMS IT policy rule

### Description

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

### Default value

The default value is True.

### Usage

Change this rule to False to prevent a user from sending SMS text messages.

Changing this rule to False does not prevent a user from receiving SMS text messages.

### Dependencies

To block incoming SMS text messages, in the Security policy group, configure the Firewall Block Incoming Messages IT policy rule.

### Minimum requirements

- Java® based BlackBerry® device
- BlackBerry® Connect™ versions 1.2, 2.0, 2.1, 4.0
- BlackBerry® Device Software version 3.6
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® and BlackBerry® Enterprise Server for Novell® GroupWise® version 4.0
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.5

### Exceptions

The BlackBerry Enterprise Server for Novell GroupWise supports this rule in BlackBerry Device Software version 4.0 or later.

## Default Browser Config UID IT policy rule

### Description

This rule specifies a unique ID for the browser configuration service book, which specifies the default browser configuration on a BlackBerry® device.

For more information about the browser configurations available on a BlackBerry device, see the Browser policy group.

### Default value

The default value is a null value.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Connect™ versions 2.1, 4.0 (internal)
- BlackBerry® Device Software version 3.6
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® and BlackBerry® Enterprise Server for Novell® GroupWise® version 4.0
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.5

### Exceptions

The BlackBerry Enterprise Server for Novell GroupWise supports this rule in BlackBerry Device Software version 4.0 or later.

## Enable Long-Term Timeout IT policy rule

### Description

This rule specifies whether a BlackBerry® device locks after a predefined period of time, regardless of user activity.

### Default values

The default value in the Default and Basic password security IT policies is null.

The default value in all other preconfigured IT policies is True.

### Usage

Configure this rule to True to force a BlackBerry device to lock automatically after 60 minutes.

### Dependencies

Use the Periodic Challenge Time IT policy rule to shorten or extend the timeout interval.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Connect™ versions 1.2, 2.0, 2.1, 4.0
- BlackBerry® Device Software version 3.6
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® and BlackBerry® Enterprise Server for Novell® GroupWise® version 4.0
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.5

### Exceptions

The BlackBerry Enterprise Server for Novell GroupWise supports this rule in BlackBerry Device Software version 4.0 or later.

## Enable WAP Config IT policy rule

### Description

This rule specifies whether a separate icon appears on a BlackBerry® device if the appropriate service books are present for the WAP Browser.

For more information about the browser configurations that are available on a BlackBerry device, see the Browser policy group.

### Default value

The default value is True.

### Usage

Change this rule to False to turn off the WAP service and hide the WAP Browser icon on a BlackBerry device.

Turning off the WAP service might turn off the ability to send and receive MMS messages if your network service provider uses the WAP service for MMS messaging.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Connect™ versions 2.1, 4.0
- BlackBerry® Device Software version 3.6
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® and BlackBerry® Enterprise Server for Novell® GroupWise® version 4.0
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.5

### Exceptions

The BlackBerry Enterprise Server for Novell GroupWise supports this rule in BlackBerry Device Software version 4.0 or later.

## Home Page Address IT policy rule

### Description

This rule specifies the BlackBerry® Browser home page.

For more information about the browser configurations that are available on a BlackBerry device, see the Browser policy group.

### Default value

The default value is a null value.

### Usage

If you do not configure this rule, a BlackBerry device uses the default home page.

### Minimum requirements

- C++-based BlackBerry device that is running BlackBerry® Device Software version 2.5
- Java® based BlackBerry device that is running BlackBerry Device Software version 3.6
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0 (internal)
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® and BlackBerry® Enterprise Server for Novell® GroupWise® version 4.0
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.5

### Exceptions

The BlackBerry Enterprise Server for Novell GroupWise supports this rule only for Java based BlackBerry devices that are running BlackBerry Device Software version 4.0 or later.

## Maximum Password Age IT policy rule

### Description

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

### Default values

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

The default value in the Basic password security IT policy is 60 days.

The default value in all other preconfigured IT policies is 30 days.

### Usage

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

### Dependencies

A BlackBerry device uses this rule only if the Password Required IT policy rule is configured to True.

### Minimum requirements

- C++-based BlackBerry device that is running BlackBerry® Device Software version 2.5
- Java® based BlackBerry device that is running BlackBerry Device Software version 3.6
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ versions 1.2, 2.0, 2.1, 4.0
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® and BlackBerry® Enterprise Server for Novell® GroupWise® version 4.0
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.5

### Exceptions

The BlackBerry Enterprise Server for Novell GroupWise supports this rule only for Java based BlackBerry devices that are running BlackBerry Device Software version 4.0 or later.

## Home Page Address Is Read-Only IT policy rule

### Description

This rule specifies whether a user can change the BlackBerry® Browser home page.

### Default value

The default value is a null value.

### Minimum requirements

- C++-based BlackBerry device that is running BlackBerry® Device Software version 2.5
- Java® based BlackBerry device that is running BlackBerry Device Software version 3.6
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0 (internal)
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® and Novell® GroupWise® version 4.0
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.5

### Exceptions

The BlackBerry Enterprise Server for Novell GroupWise supports this rule only for Java based BlackBerry devices that are running BlackBerry Device Software version 4.0 or later.

## Maximum Security Timeout IT policy rule

### Description

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

### Default values

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

The default value in the Basic password security IT policy is 30 minutes.

The default value in all other preconfigured IT policies is 10 minutes.

### Usage

By default, the maximum security timeout value that is available on a BlackBerry device is 60 minutes.

### Dependencies

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

A BlackBerry device user can specify any timeout value that is lower than the maximum value unless you configure the User Can Change Timeout IT policy rule to False.

Use the Set Password Timeout IT policy rule to specify a configure timeout value.

#### Minimum requirements

- C++-based BlackBerry device that is running BlackBerry® Device Software version 2.5
- Java® based BlackBerry device that is running BlackBerry Device Software version 3.6
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ versions 1.2, 2.0, 2.1, 4.0
- BlackBerry® Enterprise Server version 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. The permitted range is 4 through 14 characters. The maximum password length, which this rule does not control, is 32 characters.

#### Default value

The default value is a null value.

#### Dependencies

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

If the FIPS Level IT policy rule is configured to 2, by default, a BlackBerry device requires a minimum password length of 5 characters.

#### Minimum requirements

- C++-based BlackBerry device that is running BlackBerry® Device Software version 2.5
- Java® based BlackBerry device that is running BlackBerry Device Software version 3.6
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ versions 1.2, 2.0, 2.1, 4.0
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® and BlackBerry® Enterprise Server for Novell® GroupWise® version 4.0
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.5

#### Exceptions

The BlackBerry Enterprise Server for Novell GroupWise supports this rule only for Java based BlackBerry devices that are running BlackBerry Device Software version 4.0 or later.

## Password Pattern Checks IT policy rule

#### Description

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

**Default values**

The default value in the Default IT policy is No restrictions.

The default value in all other preconfigured IT policies is at least one alphabetic and one numeric character.

**Usage**

Change this rule to require At least 1 alpha and 1 numeric character.

Change this rule to require At least 1 alpha, 1 numeric, and 1 special character.

Change this rule to require At least 1 upper-case alpha, one lower-case alpha, 1 numeric, and 1 special character.

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

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

**Minimum requirements**

- C++-based BlackBerry device that is running BlackBerry® Device Software version 2.5
- Java® based BlackBerry device that is running BlackBerry Device Software version 3.6
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ versions 1.2, 2.0, 2.1, 4.0
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® and BlackBerry® Enterprise Server for Novell® GroupWise® version 4.0
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.5

**Exceptions**

The BlackBerry Enterprise Server for Novell GroupWise supports this rule only for Java based BlackBerry devices that are running BlackBerry Device Software version 4.0 or later.

## Password Required IT policy rule

**Description**

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

**Default values**

The default value in the Default IT policy is False.

The default value in all other preconfigured IT policies is True.

**Dependencies**

If the FIPS Level IT policy rule is configured to 2, by default, a user must configure a password.

**Minimum requirements**

- C++-based BlackBerry device that is running BlackBerry® Device Software version 2.5
- Java® based BlackBerry device that is running BlackBerry Device Software version 3.6
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ versions 1.2, 2.0, 2.1, 4.0
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® and BlackBerry® Enterprise Server for Novell® GroupWise® version 4.0
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.5

### Exceptions

The BlackBerry Enterprise Server for Novell GroupWise supports this rule only for Java based BlackBerry devices that are running BlackBerry Device Software version 4.0 or later.

## User Can Change Timeout IT policy rule

### Description

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

### Default value

The default value is True.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ versions 1.2, 2.0, 2.1, 4.0
- BlackBerry® Device Software version 3.6
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® and BlackBerry® Enterprise Server for Novell® GroupWise® version 4.0
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.5

### Exceptions

The BlackBerry Enterprise Server for Novell GroupWise supports this rule in BlackBerry Device Software version 4.0 or later.

## User Can Disable Password IT policy rule

### Description

This rule specifies whether a user can turn off a BlackBerry® device password.

### Default values

The default value in the Default IT policy is True.

The default value in all other preconfigured IT policies is False.

### Usage

Change this rule to False to prevent a user from turning off a BlackBerry device password.

### Dependencies

A BlackBerry device uses this rule only if the Password Required IT policy rule is configured to True.

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

### Minimum requirements

- C++-based BlackBerry device that is running BlackBerry Device Software version 2.5
- Java based BlackBerry device that is running BlackBerry Device Software version 3.6
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ versions 1.2, 2.0, 2.1, 4.0
- BlackBerry® Enterprise Server version 3.5

### Exceptions

The BlackBerry® Enterprise Server for Novell® GroupWise® supports this rule only on Java based BlackBerry devices that are running BlackBerry Device Software version 4.0 or later.

## Documents To Go policy group

### Disable Documents To Go IT policy rule

#### Description

This rule specifies whether a user can open files or attachments using the Documents To Go application on a BlackBerry® device.

#### Default value

The default value is False.

#### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.5 with the DataViz® Documents To Go application installed
- BlackBerry® Enterprise Server version 4.1 SP5

### Hide Documents To Go Communication Menus IT policy rule

#### Description

This rule specifies whether a user can register the Documents To Go application with DataViz®, check for software updates from DataViz, and use the premium edition of the DataViz Documents To Go application on a BlackBerry® device.

**Default value**

The default value is False.

**Dependencies**

If you configure the Disable Documents To Go IT policy rule to True, the BlackBerry device ignores this rule.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.5 with the DataViz Documents To Go application installed
- BlackBerry® Enterprise Server version 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 DataViz® Documents To Go application that are not available on a BlackBerry® device that is running the standard edition of the Documents To Go application.

**Default value**

The default value is False.

**Dependencies**

If you configure the Disable Documents To Go IT policy rule to True, the BlackBerry device ignores this rule.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.5 with the DataViz Documents To Go application installed
- BlackBerry® Enterprise Server version 4.1 SP5

## Email Messaging policy group

### 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.

**Default value**

The default value is False.

### Usage

If you change this rule to True, and the BlackBerry Attachment Service is connected to the BlackBerry® Enterprise Server using the BlackBerry Attachment Connector, a BlackBerry device downloads attachments automatically.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 4.2
- BlackBerry Enterprise Server version 4.0 SP6

## Attachment Viewing IT policy rule

### Description

This rule specifies whether a BlackBerry® device user can view supported attachments in messages and calendar entries.

### Default value

The default value is True.

### Usage

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 False does not prevent a user from downloading or viewing native attachments on a BlackBerry device.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 4.2 for messages and version 5.0 for calendar entries
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® and BlackBerry® Enterprise Server for Novell® GroupWise® version 4.0 SP6 for messages and version 5.0 for calendar entries
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.6 SP1

### Exceptions

The BlackBerry Enterprise Server for Novell GroupWise supports this rule in BlackBerry Device Software version 4.0 or later.

## Disable Form Submission IT policy rule

### Description

This rule specifies whether a BlackBerry® device user can send email messages that include embedded forms.

**Default value**

The default value is False.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.5
- BlackBerry® Enterprise Server version 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.

**Default value**

The default value is False.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.5
- BlackBerry® Enterprise Server version 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 received IBM® Lotus® Domino® encrypted email messages from a BlackBerry device. By default, a BlackBerry device user with support for reading IBM Lotus Domino encrypted email messages on a BlackBerry device can forward or reply to encrypted email messages which were received, decrypted, and decompressed on the device. The BlackBerry Messaging Agent for IBM Lotus Domino decrypts email messages before a BlackBerry device sends email messages to the recipient as plain text.

For more information about reading IBM Lotus Domino encrypted email messages on a BlackBerry device, see the *BlackBerry® Enterprise Solution Security Technical Overview*.

**Default value**

The default value is False.

**Usage**

If you change this rule to True, a BlackBerry device user cannot forward or reply to received IBM Lotus Domino encrypted email messages on the BlackBerry device.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.2.1
- BlackBerry® Enterprise Server version 4.1 SP3

## Disable Rich Content Email IT policy rule

**Description**

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

**Default value**

The default value is False.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.5
- BlackBerry® Enterprise Server version 4.1 SP5

## Enable Wireless Message Reconciliation IT policy rule

**Description**

This rule specifies whether a BlackBerry® device supports wireless email reconciliation.

When a user moves or deletes email messages on a BlackBerry device or in the email application on their computer, or marks messages as opened or unopened, the BlackBerry Messaging Agent reconciles the changes over the wireless network.

**Default value**

The default value is True.

**Usage**

If you configure this rule to True, or if it is not a part of the IT policy that you assigned to a user, by default, wireless email reconciliation is turned on for both the BlackBerry device and BlackBerry® Enterprise Server.

**Minimum requirements**

- C++-based BlackBerry device that is running BlackBerry® Device Software version 2.6
- Java® based BlackBerry device that is running BlackBerry Device Software version 3.6
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ versions 1.2, 2.0, 2.1, 4.0 (internal)
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® and BlackBerry® Enterprise Server for Novell® GroupWise® version 4.0

- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.6 SP1

**Exceptions**

The BlackBerry Enterprise Server for Novell GroupWise supports this rule only for Java based BlackBerry devices that are running BlackBerry Device Software version 4.0 or later.

## Inline Content Requests IT policy rule

**Description**

This rule specifies whether a BlackBerry® device user can send messages with inline content and view inline content automatically in messages received on the BlackBerry device.

**Default value**

The default value is Automatic allowed.

**Usage**

If you change this rule to Manual only, a BlackBerry device user can continue to request inline content in messages manually.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.5
- BlackBerry® Enterprise Server version 4.1 SP5

## Keep Message Duration IT policy rule

**Description**

This rule specifies the maximum time (in days) that a BlackBerry® device keeps messages. The permitted range is -1 through 180 days.

**Default value**

The default value is -1. A BlackBerry device keeps messages indefinitely.

**Usage**

Configure this rule to 0 or -1 to keep messages on a BlackBerry device indefinitely.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 4.2
- BlackBerry® Enterprise Server version 4.0 SP6

## Keep Saved Message Duration IT policy rule

### Description

This rule specifies the maximum time (in days) that a BlackBerry® device keeps saved messages. The permitted range is -1 through 180 days.

### Default value

The default value is -1. A BlackBerry device keeps saved messages indefinitely.

### Usage

Configure this rule to 0 or -1 to keep saved messages on a BlackBerry device indefinitely.

Configure this rule to -2 to delete saved messages and turn off the ability to save messages on a BlackBerry device that is running BlackBerry® Device Software versions 4.5 or later.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry Device Software version 4.2
- BlackBerry® Enterprise Server version 4.0 SP6

## Maximum Native Attachment MFH attachment size IT policy rule

### Description

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

### Default value

The default value is 3 MB.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 4.2
- BlackBerry® Enterprise Server version 4.0 SP6

## Maximum Native Attachment MFH total attachment size IT policy rule

### Description

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

**Default value**

The default value is 5 MB.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 4.2
- BlackBerry® Enterprise Server version 4.0 SP6

## Notes Native Encryption Password Timeout IT policy rule

**Description**

This rule specifies the maximum length of time (in minutes) that a BlackBerry® device stores the IBM® Lotus Notes® .id password that a user types. The permitted range is -1 through 32,767.

**Default value**

The default value is -1, which indefinitely stores the password that the user types.

**Usage**

Change this rule to 0 to never store the password that a user types on a BlackBerry device. If you do this, you should also prevent the BlackBerry® Enterprise Server from storing a copy of the password by default.

For more information on changing the BlackBerry Enterprise Server default behavior, visit [www.blackberry.com/support](http://www.blackberry.com/support) to read *Prevent the BlackBerry Enterprise Server from storing the password for decrypting IBM Lotus Notes-encrypted messages*.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.3
- BlackBerry Enterprise Server version 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 user sends from a BlackBerry® device.

**Default value**

The default value is a null value.

**Minimum requirements**

- Java® based BlackBerry device

- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 4.1.2
- BlackBerry® Enterprise Server version 4.0 SP5

## Maximum Native Attachment MTH attachment size

### Description

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

### Default value

The default value is 10,240 KB.

### Usage

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

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.5
- BlackBerry® Enterprise Server version 4.1 SP5

## Enterprise Voice Client policy group

### Disable DTMF Fallback IT policy rule

#### Description

This rule specifies whether a BlackBerry® device can use the DTMF call format for outgoing calls if the outgoing calls using a protocol format fail because of inadequate wireless coverage levels. The DTMF call format uses weaker authentication than the protocol call format.

#### Default value

The default value is False.

#### Usage

Change this rule to True to prevent outgoing calls if the protocol format cannot be used.

#### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Enterprise Server version 4.1 SP4

## Disable Enterprise Voice Client IT policy rule

### Description

This rule specifies whether enterprise voice is available on a BlackBerry® device.

### Default value

The default value is False.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Enterprise Server version 4.1 SP4

## Lock Outgoing Line IT policy rules

### Description

This rule specifies whether to prevent using the enterprise voice number for outgoing calls.

### Default value

The default value is False.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Enterprise Server version 4.1 SP4

## 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.

### Default value

The default value is False.

### Usage

This rule is obsolete in BlackBerry Enterprise Server versions 4.1 SP4 and later.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry Enterprise Server version 4.1 SP4

## Firewall policy group

### Restrict Incoming Cellular Calls IT policy rule

#### Description

This rule specifies whether a BlackBerry® device firewall blocks calls that a user receives unless the calls use a fixed dialing pattern.

This rule does not affect emergency calls.

#### Default value

The default value is a null value.

#### Usage

Type one or more fixed dialing patterns (for example, specific dialing numbers, or a set of dialing numbers with the same prefix) separated by a semi-colon.

To receive calls from numbers that are preceded by 1 or +1 only, type **+1...;1...**

To deny receiving calls using a specific pattern, append **r** to that pattern. For example, type **011...r** to deny receiving calls in the format *011NNNNNNNNNN*.

To indicate that all other patterns are denied, type **r** in the pattern list. For example, to receive calls from the number 519-555-1234 only, type **+15195551234;15195551234;5195551234;r**.

#### Dependencies

BlackBerry device users must subscribe to caller ID to use this rule.

#### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.3
- BlackBerry® Enterprise Server version 4.1 SP5

### Restrict Outgoing Cellular Calls IT policy rule

#### Description

This rule specifies whether a BlackBerry® device firewall blocks calls that a user makes unless the calls use a fixed dialing pattern.

This rule does not affect emergency calls.

#### Default value

The default value is a null value.

#### Usage

Type one or more fixed dialing patterns (for example, specific dialing numbers, or a set of dialing numbers with the same prefix) separated by a semi-colon.

To make calls to numbers that are preceded by 1 or +1 only, type **+1...;1...**

To deny making calls using a specific pattern, append **r** to that pattern. For example, type **011...r** to deny making calls in the format *011NNNNNNNNNN*.

To indicate that all other patterns are denied, type **r** in the pattern list. For example, to make calls to the number 519-555-1234 only, type **+15195551234;15195551234;5195551234;r**.

### Dependencies

A BlackBerry device user must subscribe to caller ID to use this rule.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.3
- BlackBerry® Enterprise Server version 4.1 SP5

## Global items

### Allow Browser IT policy rule

#### Description

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

#### Default value

The default value is True.

#### Usage

This rule does not affect other browsers such as the WAP browser.

For more information about the browser configurations that are available on a BlackBerry device, see the Browser policy group.

#### Minimum requirements

- C++-based BlackBerry device that is running BlackBerry® Device Software version 2.5
- Java® based BlackBerry device that is running BlackBerry Device Software version 3.6
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ versions 1.2, 2.0, 2.1, 4.0 (internal)
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® and BlackBerry® Enterprise Server for Novell® GroupWise® version 4.0
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.5

#### Exceptions

The BlackBerry Enterprise Server for Novell GroupWise supports this rule only for Java based BlackBerry devices that are running BlackBerry Device Software version 4.0 or later.

## Allow Phone IT policy rule

### Description

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

### Default value

The default value is True.

### Usage

Change this rule to False to prevent a user from making and receiving any calls except emergency calls. The phone icon remains on the BlackBerry device.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ versions 1.2, 2.0, 2.1, 4.0
- BlackBerry® Device Software version 3.6
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® version 4.0
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.5

### Exceptions

The BlackBerry® Enterprise Server for Novell® GroupWise® supports this rule in BlackBerry Device Software version 4.0 or later.

## Auto Signature IT policy rule

### Description

This rule specifies the signature that is attached automatically to outgoing email messages.

### Default value

The default value is a null value.

### Usage

Use this rule to add a disclaimer to the end of email messages that a user sends from a BlackBerry® device.

This rule is obsolete in BlackBerry® Enterprise Server version 4.1 SP2 and later.

### Minimum requirements

- BlackBerry® Desktop Software version 3.5
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® version 4.0

- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.5

**Exceptions**

The BlackBerry Enterprise Server for Microsoft Exchange supports this rule in BlackBerry Enterprise Server version 3.5 to version 4.1 SP2.

The BlackBerry® Enterprise Server for Novell® GroupWise® does not support this rule.

## Instant Messaging policy group

### 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.

**Default value**

The default value is a null value. The user can send all file types.

**Usage**

Specify the extensions of the disallowed file types in a comma-delimited format (for example, bat, exe, mp3) to prevent a user from sending specific file types.

Configure this rule to "\*" to prevent a user from sending any file type.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.2
- BlackBerry® Enterprise Server version 4.1 SP6

### Disable Emailing Conversation IT policy rule

**Description**

This rule specifies whether a user can send an instant messaging conversation in an email message from a BlackBerry® device.

**Default value**

The default value is False.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.1

- BlackBerry® Enterprise Server version 4.1 SP6

## Disable Saving Conversation IT policy rule

### Description

This rule specifies whether a user can save an instant messaging conversation to a BlackBerry® device or a media card.

### Default value

The default value is False.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.2
- BlackBerry® Enterprise Server version 4.1 SP6

## Location Based Services policy group

### Disable BlackBerry Maps IT policy rule

#### Description

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

#### Default value

The default value is False.

#### Minimum requirements

- BlackBerry® Enterprise Server version 4.0 SP6
- BlackBerry® Application Suite version 1.0

### 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 regularly. A BlackBerry device user must click **Yes** when prompted to permit location tracking on a BlackBerry device.

#### Default value

The default value is False. The default interval is 15 minutes.

#### Usage

Change this rule to True to permit a BlackBerry device user to require that a BlackBerry device reports its location to the BlackBerry Enterprise Server at regular intervals. You can use the Enterprise Location Tracking Interval IT policy rule to change the interval.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.2.2
- BlackBerry Enterprise Server version 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 user that the BlackBerry® Enterprise Server is tracking the location of the BlackBerry device.

**Default value**

The default value is "Your location is now being tracked at the server."

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.2.2
- BlackBerry Enterprise Server version 4.1 SP3

## Enterprise Location Tracking Interval IT policy rule

**Description**

This rule specifies the amount of time interval (in minutes) between location reports sent by a BlackBerry® device to the BlackBerry® Enterprise Server. The permitted range is 15 through 60 minutes.

**Default value**

The default value is 15 minutes.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.2.2
- BlackBerry Enterprise Server version 4.1 SP3

## MDS Integration Service policy group

### Disable Activation With Public BlackBerry MDS Integration Service IT policy rule

#### Description

This rule specifies whether to prevent a BlackBerry® device user from initiating a connection with the public BlackBerry MDS Integration Service.

#### Default value

The default value is False.

#### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 4.2
- BlackBerry® Enterprise Server version 4.1 SP2

### Disable MDS Runtime IT policy rule

#### Description

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

#### Default value

The default value is False.

#### Usage

Change this rule to True to prevent a user from activating the BlackBerry MDS Runtime.

#### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 4.0
- BlackBerry® Enterprise Server version 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 initiating a connection with the BlackBerry MDS Integration Service.

**Default value**

The default value is False.

**Usage**

Change this rule to True to prevent a user from initiating the BlackBerry MDS Integration Service connection.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 4.2
- BlackBerry® Enterprise Server version 4.0 SP6

## Lowest BlackBerry MDS Integration Service Security version Allowed IT policy rule

**Description**

This rule specifies the lowest security version permitted for the BlackBerry® MDS Integration Service.

**Default value**

The default value is 1.

**Usage**

Change this rule to 1 to permit a BlackBerry device that is running BlackBerry MDS Runtime version 1.1 or later to communicate with all versions of the BlackBerry MDS Integration Service.

Change this rule to 2 to permit a BlackBerry device that is running BlackBerry MDS Runtime version 1.1 or later to communicate with BlackBerry MDS Integration Service version 4.1 SP2 or later only.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 4.2
- BlackBerry® Enterprise Server version 4.0 SP6

## 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.

**Default value**

The default value is False. The BlackBerry MDS Integration Service permits unauthenticated connections from a BlackBerry device that is running BlackBerry MDS Runtime version 1.1 or later.

### Usage

If you change this rule to True, the BlackBerry MDS Integration Service does not permit unauthenticated connections from a BlackBerry device that is running BlackBerry MDS Runtime version 1.1 or later.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 4.2
- BlackBerry® Enterprise Server version 4.0 SP6

## 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 Holstered IT policy rule

#### Description

This rule specifies whether a BlackBerry® device cleans its memory while in the BlackBerry device holster.

#### Default value

The default value is False.

#### Minimum requirements

- Java® based BlackBerry device
- S/MIME Support Package for BlackBerry® smartphones version 1.5
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 3.6
- BlackBerry® Enterprise Server version 4.0 SP3

#### Exceptions

The BlackBerry® Enterprise Server for Novell® GroupWise® does not support this rule.

### Force Memory Clean When Idle IT policy rule

#### Description

This rule specifies whether a BlackBerry® device cleans its memory during periods of user inactivity.

**Default value**

The default value is False.

**Minimum requirements**

- Java® based BlackBerry device
- S/MIME Support Package for BlackBerry® smartphones version 1.5
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 3.6
- BlackBerry® Enterprise Server version 4.0 SP3

**Exceptions**

The BlackBerry® Enterprise Server for Novell® GroupWise® does not support this rule.

## Memory Cleaner Maximum Idle Time IT policy rule

**Description**

This rule specifies the maximum time (in minutes) that a BlackBerry® device can be inactive before the BlackBerry device cleans its memory. The permitted range is 1 through 60 minutes.

**Default value**

The default value is 60 minutes.

**Dependencies**

A BlackBerry device uses this rule only if you configure the Force Memory Clean When Idle IT policy rule to True.

**Minimum requirements**

- Java® based BlackBerry device
- S/MIME Support Package for BlackBerry® smartphones version 1.5
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 3.6
- BlackBerry® Enterprise Server version 4.0 SP3

**Exceptions**

The BlackBerry® Enterprise Server for Novell® GroupWise® does not support this rule.

## On-Device Help policy group

### On-Device Help Links IT policy rule

#### Description

This rule specifies links to add to the index page of the help on a BlackBerry® device.

#### Default value

The default value is a null value.

#### Usage

Specify links using the following format: *uri1\|label1\|...|uriN\|labelN..*

#### Dependencies

If you specify multiple links, you should also configure a label in the On-Device Help Group Label IT policy rule.

#### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 4.1
- BlackBerry® Enterprise Server version 4.0 SP3

### On-Device Help Group Label IT policy rule

#### Description

This rule specifies a label to use for multiple links in the help on a BlackBerry® device.

#### Default value

The default value is a null value.

#### Dependencies

Configure a group label if you specify multiple links using the On-Device Help Links IT policy rule.

#### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.1
- BlackBerry® Enterprise Server version 4.0 SP3
- BlackBerry® Application Suite version 1.0

## Password policy group

A BlackBerry® device uses the IT policy rules in the Password policy group only if, in the Device Only items, you configure the Password Required IT policy rule to True. 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 users type their BlackBerry® device passwords 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 BlackBerry device password is blackberry, the duress password is lackberryb.

If you configure this rule, the maximum number of password attempts is reduced by half. Each time a user types a password to unlock a BlackBerry device, the BlackBerry device must confirm whether the password is either the correct password or the duress password.

#### Default value

The default value is a null value.

#### Usage

Configure this rule to permit a user to notify you that a BlackBerry device might have been stolen. Instruct users how to use the duress password feature.

To prevent an unlocked BlackBerry 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.

#### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 4.0
- BlackBerry® Enterprise Server version 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 (,).

#### Default value

The default value is a null value.

## Usage

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

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 4.1
- BlackBerry® Enterprise Server version 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 user from reusing previous passwords.

### Default values

The default value in the Default and the Basic password security IT policies is 0.

The default value in all other preconfigured IT policies is 6.

### Usage

If you change this rule to 0, password checking is turned off.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ versions 1.2, 2.0, 2.1, 4.0
- BlackBerry® Device Software version 3.6
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® and BlackBerry® Enterprise Server for Novell® GroupWise® version 4.0
- BlackBerry® Enterprise Server for Microsoft® Exchange versions 3.6 and later.

### Exceptions

The BlackBerry Enterprise Server for Novell GroupWise supports this rule in BlackBerry Device Software version 4.0 or later.

## Periodic Challenge Time IT policy rule

### Description

This rule specifies the security timeout interval (in minutes) after which a BlackBerry® device locks and prompts a user to type a password, regardless of whether the BlackBerry device was active during that interval.

**Default value**

If you change the Enable Long-Term Timeout IT policy rule to True, by default the security timeout interval is turned on and set to 60 minutes.

**Usage**

Type a periodic challenge time to shorten or extend the security timeout interval to a value that is within the range of 1 to 1440 minutes.

**Dependencies**

A BlackBerry device uses this rule only if a security password is configured. To require that a user configure a security password, configure the Password Required IT policy rule to True. You can also change the User Can Change Timeout IT policy rule to False so that a user cannot change the timeout settings on a BlackBerry device.

**Minimum requirements**

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

## Set Maximum Password Attempts IT policy rule

**Description**

This rule specifies the number of password attempts that a user can make before a BlackBerry® device erases all of the application data. The permitted range is 3 through 10 attempts.

**Default value**

The default value is 10 attempts.

**Usage**

By default, the maximum number of password attempts is 10. Use this rule to lower the number of password attempts.

**Minimum requirements**

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

**Exceptions**

The BlackBerry® Enterprise Server for Novell® GroupWise® supports this rule in BlackBerry Device Software versions 4.0 and later.

## Set Password Timeout IT policy rule

### Description

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

### Default value

The default value is 2 minutes for BlackBerry® Device Software versions earlier than 4.7, and 30 minutes for BlackBerry Device Software versions 4.7 and later.

### Usage

Use this rule to change the default security timeout interval.

### Dependencies

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

If you do not change the User Can Change Timeout IT policy rule to False, the user can change the security timeout to any value.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ versions 1.2, 2.0, 2.1, 4.0
- BlackBerry Device Software version 3.6
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® and BlackBerry® Enterprise Server for Novell® GroupWise® version 4.0
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.6

### Exceptions

The BlackBerry Enterprise Server for Novell GroupWise supports this rule in BlackBerry Device Software version 4.0 or later.

## Suppress Password Echo IT policy rule

### Description

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

### Default value

The default value is True.

### Dependencies

If you configure the FIPS Level IT policy rule to 2, by default, the characters that a user types do not appear on the screen.

**Minimum requirements**

- Java® based BlackBerry® device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ versions 1.2, 2.0, 2.1, 4.0
- BlackBerry® Device Software version 3.6
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® and Novell® GroupWise® version 4.0
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.6

**Exceptions**

The BlackBerry Enterprise Server for Novell GroupWise supports this rule in BlackBerry Device Software version 4.0 or later.

## 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 .

**Default value**

The default value is False.

**Minimum requirements**

- C++-based BlackBerry device that is running BlackBerry® Device Software version 2.7
- Java® based BlackBerry device that is running BlackBerry Device Software version 4.0
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0 (internal)
- BlackBerry® Enterprise Server version 4.0

**Exceptions**

The BlackBerry® Enterprise Server for Novell® GroupWise® supports this rule only for Java based BlackBerry devices.

### Disable All Wireless Synchronization IT policy rule

**Description**

This rule specifies whether wireless data synchronization for all organizer data is turned off.

**Default value**

The default value is False.

### Usage

Change this rule to True to turn off wireless data synchronization for contact and calendar entries, email message filters, tasks, and memos. If you change this rule to True, you cannot manage software configurations as expected.

This rule does not affect wireless email reconciliation.

### Minimum requirements

- C++ based BlackBerry® device that is running BlackBerry® Device Software version 2.7
- Java® based BlackBerry device that is running BlackBerry Device Software version 4.0
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0 (internal)
- BlackBerry® Enterprise Server version 4.0

## Disable Calendar Wireless Synchronization IT policy rule

### Description

This rule specifies whether wireless data synchronization for the calendar is turned off.

### Default value

The default value is False.

### Minimum requirements

- Java® based BlackBerry® device that is running BlackBerry® Device Software version 4.0
- C++-based BlackBerry device that is running BlackBerry Device Software version 2.7
- BlackBerry® Enterprise Server version 4.0
- BlackBerry® Connect™ version 4.0 (internal)
- BlackBerry® Application Suite version 1.0

### Exceptions

The BlackBerry® Enterprise Server for Novell® GroupWise® supports this rule only for Java based BlackBerry devices.

## Disable Enterprise Activation Progress IT policy rule

### Description

This rule specifies whether the Home screen displays enterprise activation progress.

### Default value

The default value is True. Activation progress does not appear on the Home screen.

### Minimum requirements

- Java® based BlackBerry® device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 4.2
- BlackBerry® Enterprise Server version 4.0 SP6

## Disable Memopad Wireless Sync IT policy rule

### Description

This rule specifies whether wireless data synchronization for memos is turned off.

### Default value

The default value is False.

### Minimum requirements

- C++-based BlackBerry® device that is running BlackBerry® Device Software version 2.7
- Java® based BlackBerry device that is running BlackBerry Device Software version 4.0
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0 (internal)
- BlackBerry® Enterprise Server version 4.0

### Exceptions

The BlackBerry® Enterprise Server for Novell® GroupWise® supports this rule only for Java based BlackBerry devices.

## Disable Phone Call Log Wireless Synchronization IT policy rule

### Description

This rule specifies whether wireless data synchronization for call logs is turned off.

### Default value

The default value is False.

### Minimum requirements

- Java® based BlackBerry® device
- BlackBerry® Application Suite version .10
- BlackBerry® Device Software version 4.1
- BlackBerry® Enterprise Server version 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.

**Default value**

The default value is True.

**Usage**

If you change this rule to False, the BlackBerry® Enterprise Server logs all PIN messages in unencrypted format to the log file that you specify. Make sure that the log file is in a location that restricts internal and external user access.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 4.1
- BlackBerry Enterprise Server version 4.0 SP6

## Disable SMS Messages Wireless Sync IT policy rule

**Description**

This rule specifies whether wireless data synchronization for SMS text messages is turned off.

**Default value**

The default value is True.

**Usage**

If you change this rule to False, the BlackBerry® Enterprise Server logs all SMS text messages in unencrypted format to the log file that you specify. Make sure that the log file is in a location that restricts internal and external user access.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 4.1
- BlackBerry Enterprise Server version 4.0 SP6

**Exceptions**

The BlackBerry® Enterprise Server for Novell® GroupWise® supports this rule in BlackBerry Device Software versions 4.0 or later.

## Disable Task Wireless Sync IT policy rule

**Description**

This rule specifies whether wireless data synchronization for tasks is turned off.

**Default value**

The default value is False.

#### **Minimum requirements**

- C++-based BlackBerry® device that is running BlackBerry® Device Software version 2.7
- Java® based BlackBerry device that is running BlackBerry Device Software version 4.0
- BlackBerry® Connect™ version 4.0 (internal)
- BlackBerry® Application Suite version 1.0
- BlackBerry® Enterprise Server version 4.0

#### **Exceptions**

The BlackBerry® Enterprise Server for Novell® GroupWise® supports this IT policy rule only for Java based BlackBerry devices.

## **Disable Wireless Bulk Loads IT policy rule**

#### **Description**

This rule specifies whether wireless data synchronization during activation or as part of a backup and restore operation is turned off.

#### **Default value**

The default value is False.

#### **Usage**

Change this rule to True to minimize wireless data transfers when activating or updating a BlackBerry® device. A BlackBerry device must be physically connected to a computer before the data transfer starts.

If a BlackBerry device is disconnected from the computer during the initial data transfer, the BlackBerry® Desktop Software sends the remaining data over the wireless network.

#### **Minimum requirements**

- C++-based BlackBerry® device that is running BlackBerry® Device Software version 2.7
- Java® based BlackBerry device that is running BlackBerry Device Software version 4.0
- BlackBerry® Connect™ version 4.0 (internal)
- BlackBerry® Enterprise Server version 4.0

#### **Exceptions**

The BlackBerry® Enterprise Server for Novell® GroupWise® supports this rule only for Java based BlackBerry devices that are running BlackBerry Device Software versions 4.0 or later.

## 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.

#### Default value

The default value is to use all supported algorithms.

#### Usage

Specify the content ciphers that a BlackBerry device can use to encrypt PGP messages from the following list:

- AES (256-bit)
- AES (192-bit)
- AES (128-bit)
- CAST (128-bit)
- Triple DES

To maintain compatibility with most PGP clients, use Triple DES encryption and CAST. By default, a BlackBerry device is designed to encrypt email messages using Triple DES encryption if it does not know the decryption capabilities available to a recipient.

#### Dependencies

If you configure the FIPS Level IT policy rule to 2, a BlackBerry device uses AES (256-bit), AES (192-bit), AES (128-bit), and Triple DES encryption.

#### Minimum requirements

- Java® based BlackBerry device
- PGP® Support Package for BlackBerry® smartphones version 4.1
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 4.1
- BlackBerry® Enterprise Server version 4.0 SP2

#### Exceptions

The BlackBerry® Enterprise Server for Novell® GroupWise® does not support this rule.

## PGP Allowed Encrypted Attachment Mode

### Description

This rule specifies the mode for retrieving PGP® protected attachment information on a BlackBerry® device.

### Default value

The default value is Automatic. A BlackBerry device requests decrypted attachment information from the BlackBerry® Enterprise Server automatically when users open PGP protected messages that contain attachments.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.5
- BlackBerry Enterprise Server version 4.1 SP5

## PGP Allowed Encryption Type IT policy rule

### Description

This rule specifies the types of encryption that a BlackBerry® device can use with PGP® protected messaging.

### Default value

The default value is Both. The BlackBerry device uses PGP based encryption and conventional encryption.

### Usage

Change this rule to PGP key-based encryption only.

Change this rule to Conventional encryption only.

### Minimum requirements

- Java® based BlackBerry® device
- BlackBerry® Device Software version 4.6
- BlackBerry® Enterprise Server version 4.1 SP6
- PGP® Support Package for BlackBerry® smartphones version 4.0

## 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

The default value is a null value.

**Minimum requirements**

- Java® based BlackBerry Device Software device
- PGP® Support Package for BlackBerry® smartphones version 4.1
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 4.1
- BlackBerry® Enterprise Server version 4.0 SP2

**Exceptions**

The BlackBerry® Enterprise Server for Novell® GroupWise® does not support this rule.

## PGP Force Digital Signature IT policy rule

**Description**

This rule specifies whether a BlackBerry® device digitally signs all PGP® protected messages that it sends.

**Default value**

The default value is False.

**Usage**

If you apply this rule, you might override secure email policy settings on the PGP Universal Server.

**Minimum requirements**

- Java® based BlackBerry device
- PGP® Support Package for BlackBerry® smartphones version 4.1
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 4.1
- BlackBerry® Enterprise Server version 4.0 SP2

**Exceptions**

The BlackBerry® Enterprise Server for Novell® GroupWise® does not support this rule.

## PGP Force Encrypted Messages IT policy rule

**Description**

This rule specifies whether a BlackBerry® device encrypts all PGP® protected messages that it sends.

**Default value**

The default value is False.

**Usage**

If you apply this rule, you might override secure email policy settings on the PGP Universal Server.

**Minimum requirements**

- Java® based BlackBerry device
- PGP® Support Package for BlackBerry® smartphones version 4.1
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 4.1
- BlackBerry® Enterprise Server version 4.0 SP2

**Exceptions**

The BlackBerry® Enterprise Server for Novell® GroupWise® does not support this rule.

## PGP Minimum Strong DH Key Length IT policy rule

**Description**

This rule specifies the minimum Diffie-Hellman key size (in bits) to use with PGP® protected messages. The permitted range is 512 through 4096 bits.

**Default value**

The default value is 1024 bits.

**Dependencies**

Configure the Disable Weak Certificate Use IT policy rule to True to prevent a user from sending email messages using certificates that have corresponding weak public keys.

**Minimum requirements**

- Java® based BlackBerry® device
- PGP® Support Package for BlackBerry® smartphones version 4.1
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 4.1
- BlackBerry® Enterprise Server version 4.0 SP2

**Exceptions**

The BlackBerry® Enterprise Server for Novell® GroupWise® does not support this rule.

## PGP Minimum Strong DSA Key Length IT policy rule

**Description**

This rule specifies the minimum DSA key size (in bits) to use with PGP® protected messages. The permitted range is 512 through 1024 bits.

**Default value**

The default value is 1024 bits.

### Dependencies

Configure the Disable Weak Certificate Use IT policy rule to True to prevent a user from sending email messages using certificates that have corresponding weak public keys.

### Minimum requirements

- Java® based BlackBerry® device
- PGP® Support Package for BlackBerry® smartphones version 4.1
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 4.1
- BlackBerry® Enterprise Server version 4.0 SP2

### Exceptions

The BlackBerry® Enterprise Server for Novell® GroupWise® does not support this rule.

## PGP Minimum Strong RSA Key Length IT policy rule

### Description

This rule specifies the minimum RSA® key size (in bits) to use with PGP® protected messages. The permitted range is 512 through 4096 bits.

### Default value

The default value is 1024 bits.

### Dependencies

Configure the Disable Weak Certificate Use IT policy rule to True to prevent users from sending email messages using certificates that have corresponding weak public keys.

### Minimum requirements

- Java® based BlackBerry® device
- PGP® Support Package for BlackBerry® smartphones version 4.1
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 4.1
- BlackBerry® Enterprise Server version 4.0 SP2

### Exceptions

The BlackBerry® Enterprise Server for Novell® GroupWise® does not support this rule.

## PGP Universal Enrollment Method IT policy rule

### Description

This rule specifies the method that users must use to enroll with the PGP® Universal Server from a BlackBerry® device.

**Default value**

The default value is Email-based enrolment. Users are prompted to type their email address.

**Usage**

Change this rule to Domain username/password enrolment to prompt users to type their user name and password.

Users must submit their enrollment information before sending and receiving PGP protected messages on a BlackBerry device.

**Minimum requirements**

- Java® based BlackBerry device
- PGP® Support Package for BlackBerry® smartphones version 4.1
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 4.1
- BlackBerry® Enterprise Server version 4.0 SP2

**Exceptions**

The BlackBerry® Enterprise Server for Novell® GroupWise® does not support this rule.

## PGP Universal Policy Cache Timeout IT policy rule

**Description**

This rule specifies the length of time (in hours) that a BlackBerry® device caches the PGP® Universal Server address. The permitted range is 4 through 48 hours.

**Default value**

The default value is 24 hours.

**Minimum requirements**

- Java® based BlackBerry device
- PGP® Support Package for BlackBerry® smartphones version 4.1
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 4.1
- BlackBerry® Enterprise Server version 4.0 SP2

**Exceptions**

The BlackBerry® Enterprise Server for Novell® GroupWise® does not support this rule.

## PGP Universal Server Address IT policy rule

**Description**

This rule specifies the address of your organization's PGP® Universal Server. The PGP Universal Server applies secure email policies that the PGP Universal Server administrator configures.

**Default value**

The default value is a null value.

**Usage**

Configure this rule to require the user to register with the PGP Universal Server. When registered, a BlackBerry® device with the PGP Support Package for BlackBerry® smartphones enforces compliance with the secure email policies for all email messages.

**Dependencies**

If you configure this rule, a user must install the PGP Support Package for BlackBerry smartphones on the BlackBerry device.

**Minimum requirements**

- Java® based BlackBerry device
- PGP® Support Package for BlackBerry® smartphones version 4.1
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 4.1
- BlackBerry® Enterprise Server version 4.0 SP2

**Exceptions**

The BlackBerry® Enterprise Server for Novell® GroupWise® does not support this rule.

## RIM Value-Added Applications policy group

### Disable BlackBerry Wallet IT policy rule

**Description**

This rule specifies whether to prevent BlackBerry® Wallet from running on a BlackBerry device.

**Default value**

The default value is False.

**Minimum requirements**

- BlackBerry® Enterprise Server version 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.

**Default value**

The default value is False.

**Minimum requirements**

- BlackBerry® Enterprise Server version 4.1 SP6

## Disable Lotus Connections IT policy rule

**Description**

This rule specifies whether to prevent IBM® Lotus® Connections from running on a BlackBerry® device.

**Default value**

The default value is False.

**Minimum requirements**

- BlackBerry® Enterprise Server version 4.1 SP6

## Lotus Connections Activities Server IT policy rule

**Description**

This rule specifies the address of the server that hosts the IBM® Lotus® Connections Activities component.

**Default value**

The default value is a null value.

**Usage**

If you configure this rule, users can use the specified server address only.

If you do not configure this rule, users must specify the server address manually.

**Minimum requirements**

- BlackBerry® Enterprise Server version 4.1 SP6

## Lotus Connections Blogs Server IT policy rule

**Description**

This rule specifies the address of the server that hosts the IBM® Lotus® Connections Blogs component.

**Default value**

The default value is a null value.

**Usage**

If you configure this rule, users can use the specified server address only.

If you do not configure this rule, users must specify the server address manually.

**Minimum requirements**

- BlackBerry® Enterprise Server version 4.1 SP6

## Lotus Connections Communities Server IT policy rule

**Description**

This rule specifies the address of the server that hosts the IBM® Lotus® Connections Communities component.

**Default value**

The default value is a null value.

**Usage**

If you configure this rule, users can use the specified server address only.

If you do not configure this rule, users must specify the server address manually.

**Minimum requirements**

- BlackBerry® Enterprise Server version 4.1 SP6

## Lotus Connections Dogear Server IT policy rule

**Description**

This rule specifies the address of the server that hosts the IBM® Lotus® Connections Dogear component.

**Default value**

The default value is a null value.

**Usage**

If you configure this rule, users can use the specified server address only.

If you do not configure this rule, users must specify the server address manually.

**Minimum requirements**

- BlackBerry® Enterprise Server version 4.1 SP6

## Lotus Connections Profiles Server IT policy rule

### Description

This rule specifies the address of the server that hosts the IBM® Lotus® Connections Profiles component.

### Default value

The default value is a null value.

### Usage

If you configure this rule, users can use the specified server address only.

If you do not configure this rule, users must specify the server address manually.

### Minimum requirements

- BlackBerry® Enterprise Server version 4.1 SP6

## S/MIME Application policy group

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

## 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

The default value is a null value.

### Usage

Use a null value if your organization does not use an Entrust Entelligence messaging server.

### Minimum requirements

- Java® based BlackBerry® device
- S/MIME Support Package for BlackBerry® smartphones version 4.0
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 4.0

- BlackBerry® Enterprise Server version 4.0 SP3

**Exceptions**

The BlackBerry® Enterprise Server for Novell® GroupWise® does not support this rule.

## S/MIME Allowed Content Ciphers IT policy rule

**Description**

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

**Default value**

The default value is to use all supported algorithms.

**Usage**

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

**Dependencies**

If you configure the FIPS Level IT policy rule to 2, a BlackBerry device uses AES (256-bit), AES (192-bit), AES (128-bit), and Triple DES encryption.

**Minimum requirements**

- Java® based BlackBerry device
- S/MIME Support Package for BlackBerry® smartphones version 1.5
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 3.6
- BlackBerry® Enterprise Server version 4.0 SP3

**Exceptions**

The BlackBerry® Enterprise Server for Novell® GroupWise® does not support this rule.

## 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.

**Default value**

The default value is Automatic. A BlackBerry device requests decrypted attachment information from the BlackBerry® Enterprise Server automatically when a user opens S/MIME-protected messages that contain attachments.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.5
- BlackBerry Enterprise Server version 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 messaging.

**Default value**

The default value is Both. The BlackBerry device uses certificate-based encryption and password-based encryption.

**Usage**

Configure this rule to Certificate-based encryption only.

Configure this rule to Password-based encryption only.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.6
- BlackBerry® Enterprise Server version 4.1 SP6
- S/MIME Support Package for BlackBerry® smartphones version 4.0

## S/MIME Blind Copy Address IT policy rule

**Description**

This rule specifies an email address that is added as a BCC recipient to all sent S/MIME-protected messages.

**Default value**

The default value is a null value.

**Minimum requirements**

- Java® based BlackBerry® device
- S/MIME Support Package for BlackBerry® smartphones version 1.5
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 3.6

- BlackBerry® Enterprise Server version 4.0 SP3

**Exceptions**

The BlackBerry® Enterprise Server for Novell® GroupWise® does not support this rule.

## S/MIME Force Digital Signature IT policy rule

**Description**

This rule specifies whether a BlackBerry® device sends all S/MIME-protected messages digitally signed.

**Default value**

The default value is False.

**Minimum requirements**

- Java® based BlackBerry device
- S/MIME Support Package for BlackBerry® smartphones version 1.5
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 3.6
- BlackBerry® Enterprise Server version 4.0 SP3

**Exceptions**

The BlackBerry Enterprise Server for Novell® GroupWise® does not support this rule.

## S/MIME Force Encrypted Messages IT policy rule

**Description**

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

**Default value**

The default value is False.

**Minimum requirements**

- Java® based BlackBerry device
- S/MIME Support Package for BlackBerry® smartphones version 1.5
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 3.6
- BlackBerry® Enterprise Server version 4.0 SP3

**Exceptions**

The BlackBerry® Enterprise Server for Novell® GroupWise® does not support this rule.

## S/MIME Force Smartcard Use IT policy rule

### Description

This rule specifies whether all operations that use certificates on a BlackBerry® device must be performed while the device is attached to a BlackBerry® Smart Card Reader.

### Default value

The default value is False.

### Minimum requirements

- Java® based BlackBerry device
- S/MIME Support Package for BlackBerry® smartphones version 1.5
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 3.6
- BlackBerry® Enterprise Server version 4.0 SP3

### Exceptions

The BlackBerry® Enterprise Server for Novell® GroupWise® does not support this rule.

## S/MIME Minimum Strong DH Key Length IT policy rule

### Description

This rule specifies the minimum Diffie-Hellman key size (in bits) to use with S/MIME-protected messages. The permitted range is 512 through 4096 bits.

### Default value

The default value is 1024 bits.

### Minimum requirements

- Java® based BlackBerry® device
- S/MIME Support Package for BlackBerry® smartphones version 1.5
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 3.6
- BlackBerry® Enterprise Server version 4.0 SP3

### Exceptions

The BlackBerry® Enterprise Server for Novell® GroupWise® does not support this rule.

## S/MIME Minimum Strong ECC Key Length IT policy rule

### Description

This rule specifies the minimum ECC key size (in bits) to use with S/MIME-protected messages. The permitted range is 163 through 571 bits.

### Default value

The default value is 163 bits.

### Minimum requirements

- Java® based BlackBerry® device
- S/MIME Support Package for BlackBerry® smartphones version 1.5
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 3.6
- BlackBerry® Enterprise Server version 4.0 SP3

### Exceptions

The BlackBerry® Enterprise Server for Novell® GroupWise® does not support this rule.

## S/MIME Minimum Strong DSA Key Length IT policy rule

### Description

This rule specifies the minimum DSA key size (in bits) to use with S/MIME-protected messages. The permitted range is 512 through 1024 bits.

### Default value

The default value is 1024 bits.

### Minimum requirements

- Java® based BlackBerry® device
- S/MIME Support Package for BlackBerry® smartphones version 1.5
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 3.6
- BlackBerry® Enterprise Server version 4.0 SP3

### Exceptions

The BlackBerry® Enterprise Server for Novell® GroupWise® does not support this rule.

## S/MIME Minimum Strong RSA Key Length IT policy rule

### Description

This rule specifies the minimum RSA® key size (in bits) to use with S/MIME-protected messages. The permitted range is 512 through 4096 bits.

### Default value

The default value is 1024 bits.

### Minimum requirements

- Java® based BlackBerry® device
- S/MIME Support Package for BlackBerry® smartphones version 1.5
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 3.6
- BlackBerry® Enterprise Server version 4.0 SP3

### Exceptions

The BlackBerry® Enterprise Server for Novell® GroupWise® does not support this rule.

## 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 that is used for the email addresses contained in certificates that are issued within your organization.

### Default value

The default value is a null value.

### Usage

Consider configuring this rule to True if your organization's certificates contain a long-lived email address but the users typically send email messages from a short-lived email address with the same user name, but a different domain name.

A BlackBerry® device uses both the short-lived and long-lived email address when searching for certificates to use with secure email messages.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 4.2
- BlackBerry® Enterprise Server version 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 the PGP® key that was used to sign the email message.

**Default value**

The default value is False.

**Usage**

Consider changing this rule to True if your organization's certificates contain email addresses that are different from those that users typically use to send email messages.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 4.2
- BlackBerry® Enterprise Server version 4.0 SP6

## 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).

**Default value**

The default value is True.

**Minimum requirements**

- Java® based BlackBerry® device

- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0 (internal)
- BlackBerry® Device Software version 3.6
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® and BlackBerry® Enterprise Server for Novell® GroupWise® version 4.0
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.6

**Exceptions**

The BlackBerry Enterprise Server for Novell GroupWise supports this rule in BlackBerry Device Software version 4.0 or later.

## Allow Internal Connections IT policy rule

**Description**

This rule specifies whether applications, including third-party applications, can initiate internal connections (for example, to the BlackBerry® MDS Connection Service).

**Default value**

The default value is True.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0 (internal)
- BlackBerry® Device Software version 3.6
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® and BlackBerry® Enterprise Server for Novell® GroupWise® version 4.0
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.6

**Exceptions**

The BlackBerry Enterprise Server for Novell GroupWise supports this rule in BlackBerry Device Software version 4.0 or later.

## Allow Outgoing Call When Locked IT policy rule

**Description**

This rule specifies whether users can place calls while a BlackBerry® device is locked.

**Default value**

The default value is False.

**Minimum requirements**

- Java® based BlackBerry device

- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0 (internal)
- BlackBerry® Device Software version 3.6
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® version 4.0
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.6

## Allow Resetting of Idle Timer IT policy rule

### Description

This rule specifies whether a BlackBerry® device permits third-party applications to reset the inactivity timeout value on a BlackBerry device, bypassing the security timeout value.

### Default value

The default value is False.

### Minimum requirements

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

### Default value

The default value is True.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.2.2
- BlackBerry® Enterprise Server version 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.

### Default value

The default value is False.

### Usage

Change this rule to True to cache the smart card password for the period of time that the private key timeout sets. The memory cleaner application deletes the password when the timeout expires.

### Dependencies

If you configure this rule, you should also configure the Key Store Password Maximum Timeout IT policy rule.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 4.0
- BlackBerry® Enterprise Server version 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 simultaneously.

### Default value

The default value is False.

### Usage

Opening internal and external connections simultaneously might present a security issue because applications can collect data from inside the firewall and send it outside the firewall without any auditing.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0 (internal)
- BlackBerry® Device Software version 3.6
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® and BlackBerry® Enterprise Server for Novell® GroupWise® version 4.0
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.6

### Exceptions

The BlackBerry Enterprise Server for Novell GroupWise supports this rule in BlackBerry Device Software version 4.0 or later.

## 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.

### Default value

The default value is True.

### Usage

This rule is obsolete in BlackBerry® Enterprise Server for Microsoft® Exchange version 3.6 SP2. In later versions of BlackBerry® Enterprise Server for Microsoft® Exchange, use the Interprocess Communication application control policy rule to specify whether applications can access the persistent store API.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 3.6
- BlackBerry Enterprise Server for Microsoft Exchange version 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.

### Default value

The default value is True.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 3.6
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® and BlackBerry® Enterprise Server for Novell® GroupWise® version 4.0
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.6

### Exceptions

The BlackBerry Enterprise Server for Novell GroupWise supports this rule in BlackBerry Device Software version 4.0 or later.

## Certificate Status Maximum Expiry Time IT policy rule

### Description

This rule specifies the maximum length of time (in hours) that a certificate status can remain on a BlackBerry® device before it should be updated in the key store on the BlackBerry device and in the certificate synchronization tool of the BlackBerry® Desktop Manager. The permitted range is 1 through 4380 hours.

**Default value**

The default value is a null value. The certificate status can remain on the BlackBerry device indefinitely.

**Minimum requirements**

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

## Content Protection Strength IT policy rule

**Description**

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

**Default values**

The default value in the Advanced security and Advanced security (disallow application downloads) IT policies is strong.

The default value in all other preconfigured IT policies is a null value.

**Usage**

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

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

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

**Dependencies**

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

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

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0

- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 4.0
- BlackBerry® Enterprise Server version 4.0

## Desktop Backup IT policy rule

### Description

This rule specifies which BlackBerry® device databases are backed up by the BlackBerry® Desktop Software.

### Default value

The default value is All databases.

### Usage

Change this rule to Minimal subset of databases to back up a minimal set of BlackBerry device databases, including databases that some desktop components, such as the certificate synchronization tool of the BlackBerry® Desktop Manager, require access to.

Change this rule to No databases to prevent the backup of BlackBerry device databases.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 4.0
- BlackBerry® Enterprise Server version 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 sent between a BlackBerry device and the BlackBerry® Enterprise Server.

### Default value

The default value is False. A BlackBerry device and the BlackBerry Enterprise Server can use the Triple DES algorithm and the AES algorithm to encrypt and decrypt data that they send between each other.

### Usage

Change this rule to True to require that a BlackBerry device and the BlackBerry Enterprise Server use the AES algorithm to encrypt and decrypt data that they send between them.

### Minimum requirements

- Java® based BlackBerry device

- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0 (internal)
- BlackBerry® Device Software version 4.0
- BlackBerry Enterprise Server version 4.0

## 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.

### Default value

The default value is False.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 4.0
- BlackBerry® Enterprise Server version 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 supported BlackBerry device.

### Default value

The default value is False.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 4.2
- BlackBerry® Enterprise Server version 4.0 SP6

## Disable Forwarding Between Services IT policy rule

### Description

This rule specifies whether to prevent a BlackBerry® device user from forwarding or replying to a message on a BlackBerry device using an email account or messaging service that is associated with a BlackBerry® Enterprise Server or BlackBerry® Internet Service that is different from the service that delivered the original message.

### Usage

Use this rule to prevent forwarding or replying to a PIN message with an email message, or replying to an email message with a PIN message.

### Default value

The default value is False.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 4.0
- BlackBerry Enterprise Server version 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.

### Default value

The default value is False.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.2
- BlackBerry® Enterprise Server version 4.1 SP4

## Disable GPS IT policy rule

### Description

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

### Default value

The default value is False.

### Usage

Change this rule to True to turn off the GPS feature and prevent applications on a BlackBerry device from accessing it.

### Dependencies

If you change this rule to True, BlackBerry® Maps does not work and applications cannot access the GPS APIs for the BlackBerry device. This rule overrides the Is Access to the GPS API Allowed application control policy rule setting.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.3
- BlackBerry® Enterprise Server version 4.1 SP5

## Disable Invalid Certificate Use IT policy rule

### Description

This rule specifies whether to prevent a user from sending an email message from a BlackBerry® device using an expired or invalid certificate.

### Default value

The default value is False. A BlackBerry device warns the user that the certificate is expired or invalid, but does not prevent the user from using the certificate.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 3.6
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® and BlackBerry® Enterprise Server for Novell® GroupWise® version 4.0
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.6

### Exceptions

The BlackBerry Enterprise Server for Novell GroupWise supports this rule in BlackBerry Device Software version 4.0 or later.

## Disable IP Modem IT policy rule

### Description

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

### Default value

The default value is False.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 4.0
- BlackBerry® Enterprise Server version 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.

### Default value

The default value is False.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.0
- BlackBerry® Enterprise Server version 4.0
- BlackBerry® Connect™ version 4.0

## Disable Key Store Low Security IT policy rule

### Description

This rule specifies whether to prevent the BlackBerry® device user from setting the key store security level to Low.

### Default setting

The default setting is False.

### Usage

Change this IT policy rule to True to require the next highest level of key store security automatically.

For BlackBerry devices that are running BlackBerry® Device Software version 3.6, the next highest security level is High. For BlackBerry devices that are running BlackBerry Device Software version 4.0 or later, the next highest security level is Medium.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ Transport Stack version 4.0
- BlackBerry Device Software version 3.6
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® and BlackBerry® Enterprise Server for Novell® GroupWise® version 4.0

- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.6

**Exceptions**

The BlackBerry Enterprise Server for Novell GroupWise supports this rule in BlackBerry Device Software version 4.0 or later.

## Disable Media Manager FTP Access

**Description**

This rule specifies whether applications can access the file transfer protocol channel from the media manager tool of the BlackBerry® Desktop Manager.

**Default value**

The default value is False.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Connect™ version 4.0 (internal)
- BlackBerry® Device Software version 4.2
- BlackBerry® Enterprise Server version 4.0 SP6

**Exceptions**

The BlackBerry® Enterprise Server for Novell® GroupWise® does not support this rule.

## Disable Message Normal Send IT policy rule

**Description**

This rule specifies whether to prevent a BlackBerry® device user from sending email messages that are not protected by additional secure messaging technology.

A BlackBerry device and the BlackBerry® Enterprise Server encrypt data sent between them automatically. This rule prevents a BlackBerry device from sending messages that are not encrypted when the BlackBerry Enterprise Server forwards them to the message recipients.

**Default value**

The default value is False.

**Usage**

If you change this rule to True, to send email messages the user must install the S/MIME Support Package for BlackBerry® smartphones or the PGP® Support Package for BlackBerry® smartphones. You must also turn on S/MIME message processing on the BlackBerry® Enterprise Server, or configure the PGP Universal Server Address IT policy rule.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 3.6
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® and BlackBerry® Enterprise Server for Novell® GroupWise® version 4.0
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.6

### Exceptions

The BlackBerry Enterprise Server for Novell GroupWise supports this rule in BlackBerry Device Software version 4.0 or later.

## 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 the PGP® Support Package for BlackBerry® smartphones.

### Default value

The default value is False.

### Usage

If you change this rule to True, to send PIN messages the user must install the S/MIME Support Package for BlackBerry smartphones or the PGP Support Package for BlackBerry smartphones on a BlackBerry device. You must also turn on S/MIME message processing on the BlackBerry® Enterprise Server, or configure the PGP Universal Server Address IT policy rule to permit PGP message processing.

To turn off all PIN messaging, configure the Allow Peer-to-Peer Messages IT policy rule to False.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 3.6
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® and BlackBerry® Enterprise Server for Novell® GroupWise® version 4.0
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.6

### Exceptions

The BlackBerry Enterprise Server for Novell GroupWise supports this rule in BlackBerry Device Software version 4.0 or later.

## 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 (for example, the file system).

### Default value

The default value is False.

### Usage

Configure this rule only if you require that sensitive data does not persist in plain text form on a BlackBerry® device.

If you change this rule to True, a BlackBerry device writes information about the application in the event log and resets, returning the BlackBerry device to a known valid state.

**Attention:** Not all applications on the BlackBerry device work if you change this rule to True.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 4.0
- BlackBerry® Enterprise Server version 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.

### Default value

The default value is False.

### Minimum requirements

- 
- Java® based BlackBerry® device
- BlackBerry® Enterprise Server version 4.1 SP4
- BlackBerry® Application Suite version 1.0

## Disable Public Social Networking Applications IT policy rule

### Description

This rule specifies whether a user can install public social networking applications on a BlackBerry® device to access public social networking services (for example, Facebook®).

**Default value**

The default value is False.

**Minimum requirements**

- Java® based BlackBerry® device
- BlackBerry® Enterprise Server version 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.

**Default value**

The default value is Radio not disabled when USB device is connected. The wireless transceiver remains on.

**Usage**

Change this rule to Radio disabled when USB device is connected to turn off the wireless transceiver while the BlackBerry device is connected to a USB device.

Change this rule to Radio disabled when connected USB device enumerates to turn off the wireless transceiver only when a connected USB device (for example, a computer) sends standard USB requests to communicate with a BlackBerry device.

**Dependencies**

Only USB enabled BlackBerry devices support this rule.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 4.0
- BlackBerry® Enterprise Server version 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.

**Default value**

The default value is False. A BlackBerry device warns the user that the certificate is revoked, but it does not prevent the user from using the certificate.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 3.6
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® and Novell® GroupWise® version 4.0
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.6

### Exceptions

The BlackBerry Enterprise Server for Novell GroupWise supports this rule in BlackBerry Device Software version 4.0 or later.

## Disable Smart Password Entry IT policy rule

### Description

This rule specifies whether to prevent a user from using smart password entry when using two-factor authentication.

If a user uses two-factor authentication and a BlackBerry® device password or authentication password is numeric, with smart password entry, the BlackBerry device remembers whether the last password typed was numeric. If the password was numeric, the next time that the user types the password, the user does not have to press the Alt key to type the numbers.

### Default value

The default value is False. A BlackBerry device stores the user's numeric passwords, and a user can use smart password entry on the BlackBerry device when using two-factor authentication.

### Usage

If you change this rule to True, a BlackBerry device deletes any knowledge of the user's numeric passwords if the user is currently using smart password entry.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 4.2
- BlackBerry® Enterprise Server version 4.0 SP6

## Disable Stale Certificate Status Checks IT policy rule

### Description

This rule specifies whether a BlackBerry® device displays warnings and indicators if the user receives an email message that includes a certificate with a stale status.

**Default value**

The default value is False

**Usage**

If you change this rule to True, a BlackBerry device does not display warnings and indicators of about stale certificate status. Consider changing this rule to True if your organization uses a PKI that does not update the status of certificates.

**Dependencies**

If you change this rule to True, a BlackBerry device ignores the Certificate Status Maximum Expiry Time IT policy rule and the status of certificates on the BlackBerry device never expires.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 4.2
- BlackBerry® Enterprise Server version 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.

**Default value**

The default value is False. A BlackBerry device warns the user that the certificate has a stale status, but it does not prevent the user from using the certificate.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 4.0
- BlackBerry® Enterprise Server version 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.

**Default value**

The default value is False. A BlackBerry device warns the user that the certificate is not trusted, but it does not prevent the user from using the certificate.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 3.6
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® and Novell® GroupWise® version 4.0
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.6

**Exceptions**

The BlackBerry Enterprise Server for Novell GroupWise supports this rule in BlackBerry Device Software version 4.0 or later.

## 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.

**Default value**

The default value is False. A BlackBerry device warns the user that the certificate could not be verified, but it does not prevent the user from using the certificate.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 4.0
- BlackBerry® Enterprise Server version 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.

**Default value**

The default value is False.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 4.0
- BlackBerry® Enterprise Server version 4.0

## Disable USB Mass Storage IT policy rule

**Description**

This rule specifies whether USB mass storage is turned on.

**Default values**

The default value in the Advanced security and the Advanced security (disallow application downloads) IT policies is True.

The default value in all other preconfigured IT policies is False.

**Usage**

If you change this rule to True, a BlackBerry® device cannot access an external file system that is connected to the USB port. This means that the ability to transfer files to an external file system using the Roxio® Media Manager with the BlackBerry® Desktop Manager versions 4.2.2 and 4.3 is turned off.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.2
- BlackBerry® Enterprise Server version 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.

**Default value**

The default value is False. A BlackBerry device warns the user that the corresponding public key is weak, but it does not prevent the user from using the certificate.

**Usage**

Use the IT policy rules that are provided for the TLS application, the WTLS application, the S/MIME Support Package for BlackBerry® smartphones, or the PGP® Support Package for BlackBerry® smartphones.

Configure the minimum strengths for the RSA®, DSA, ECC, and Diffie-Hellman algorithm key lengths.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 3.6
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® and Novell® GroupWise® version 4.0
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.6

### Exceptions

The BlackBerry Enterprise Server for Novell GroupWise supports this rule in BlackBerry Device Software version 4.0 or later.

## Disallow Third Party Application Downloads IT policy rule

### Description

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

### Default values

The default value in the Medium password security (disallow application downloads) and the Advanced security (disallow application downloads) IT policies is True.

The default value in all other preconfigured IT policies is False.

### Usage

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

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

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ versions 2.1, 4.0
- BlackBerry® Device Software version 3.6
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® and BlackBerry® Enterprise Server for Novell® GroupWise® version 4.0
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.6

### Exceptions

The BlackBerry Enterprise Server for Novell GroupWise supports this rule in BlackBerry Device Software version 4.0 or later.

## 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 an external file system, such as an external memory device.

### Default values

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

The default value in the Advanced security IT policy is Encrypt to user password (excluding multimedia directories).

The default value in all other preconfigured IT policies is a null value.

### Usage

You can use this rule to require that a BlackBerry device encrypt an external file system, either including or excluding multimedia directories. You cannot use this rule to encrypt files that a BlackBerry device user transfers to the external memory device manually (for example, from a USB mass storage device).

The external memory device stores the master keys for the media card. A BlackBerry device is designed to use those master keys to decrypt and encrypt files on the external memory device. A BlackBerry device is designed to use the BlackBerry device key, a user-provided password, or both to encrypt the master keys.

Change this rule to Encrypt to User Password (excluding multimedia directories) if the file system requires encryption with a user-provided password.

Change this rule to Encrypt to User Password (including multimedia directories) if the file system requires encryption with a user-provided password.

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

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

Change this rule to Encrypt to User Password and Device Key (excluding multimedia directories) if the file system requires encryption with a user-provided password and a BlackBerry device key.

Change this rule to Encrypt to User Password and Device Key (including multimedia directories) if the file system requires encryption with a user-provided password and the BlackBerry device key.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 4.2
- BlackBerry® Enterprise Server version 4.0 SP6

## FIPS Level IT policy rule

### Description

This rule specifies the level of FIPS compliance that your organization requires.

### Default value

The default value is FIPS 140-2 Level 1 compliance.

### Usage

This rule is obsolete in BlackBerry® Enterprise Server versions 4.1 SP3 and later and BlackBerry® Device Software versions 4.2.1 and later.

FIPS 140-2 Level 1 compliance affects the BlackBerry® Cryptographic Kernel, which is the embedded cryptographic module required for basic operation of a BlackBerry device.

FIPS 140-2 Level 2 compliance affects only the BlackBerry Device Software. It does not result in a BlackBerry device meeting FIPS 140-2 Level 2 hardware security requirements.

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.

### Dependencies

If you change this rule to 2, the following additional IT policy rules are configured:

- Password Required is configured to True
- Minimum Password Length is configured to 5
- Suppress Password Echo is configured to True
- PGP® Allowed Content Ciphers is configured to AES (256-bit), AES (192-bit), AES (128-bit), Triple DES
- S/MIME Allowed Content Ciphers is configured to AES (256-bit), AES (192-bit), AES (128-bit), Triple DES
- TLS Restrict FIPS Ciphers is configured to True
- Disallow Third Party Application Download is configured to True

### Minimum requirements

- Java® based BlackBerry device
- For FIPS Level 1 compliance, BlackBerry Device Software version 3.3
- For FIPS Level 2 compliance, BlackBerry Device Software version 4.0
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0
- BlackBerry Enterprise Server version 4.0

### Exceptions

The BlackBerry® Enterprise Server for Novell® GroupWise® supports this rule in BlackBerry Device Software version 4.0 to version 4.2.1.

## Firewall Block Incoming Messages IT policy rule

### Description

This rule specifies whether the BlackBerry® device firewall prevents the BlackBerry device from processing specific types of incoming messages, including SMS text messages, MMS messages, public and organization-specific PIN messages, and BlackBerry® Internet Service messages.

**Note:** You use the default PIN encryption key to send public PIN messages that are known to all BlackBerry devices. A BlackBerry device with an organization-specific PIN encryption key can only send and receive organization-specific PIN messages with other BlackBerry devices within your organization's network that use the same PIN encryption key.

### Default value

The default value is a null value.

### Usage

If you configure this rule, a BlackBerry device blocks the specified types of incoming messages at the firewall and does not notify the user that those types of messages were received.

A user can specify whether to block public PIN messages on a BlackBerry device. A user cannot specify whether to block organization-specific PIN messages on a BlackBerry device.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 4.2
- BlackBerry® Enterprise Server version 4.0 SP6

## Firewall Whitelist Addresses IT policy rule

### Description

This rule specifies the list of email addresses that the BlackBerry® device firewall allows. A BlackBerry device receives messages from these email addresses even if the user blocks all incoming messages on a BlackBerry device.

### Default value

The default value is a null value.

### Usage

Specify email addresses with wildcard characters (for example, \*@organization.com) to allow email messages from a specific domain.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.5

- BlackBerry® Enterprise Server version 4.1 SP5

## Force Content Protection Of Master Keys IT policy rule

### Description

This rule specifies whether content protection for master keys that a BlackBerry® device stores is turned on.

### Default value

The default value is False.

### Usage

Content protection is designed to encrypt the master encryption keys on a BlackBerry device using 256-bit AES, and to store them in the BlackBerry device memory.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 4.1
- BlackBerry® Enterprise Server version 4.0 SP3

## Force Include Address Book In Content Protection IT policy rule

### Description

This rule specifies whether the address book on a BlackBerry® device is encrypted when content protection is turned on.

By default, the content protection feature on a BlackBerry device is designed to encrypt the user data on the BlackBerry device when it is locked, but the user can choose to turn off content protection for the address book.

### Default value

The default value is False. Call display and Bluetooth® contacts transfer work when the BlackBerry device is locked and content protection is turned on.

### Usage

Change this rule to True to require that content protection includes contacts when a BlackBerry device is locked. In the General Security Options, a user cannot change the Include Address Book field. Call display and Bluetooth contacts transfer do not work when the BlackBerry device is locked.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 4.2
- BlackBerry® Enterprise Server version 4.0 SP6

## Force LED Blinking When Microphone Is On IT policy rule

### Description

This rule specifies whether a BlackBerry® device LED flashes when the microphone is on (for example, during a call or when recording a voice message).

### Default value

The default value is False.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.1
- BlackBerry® Enterprise Server version 4.0 SP3

## Force Lock When Holstered IT policy rule

### Description

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

### Default values

The default value in the Default and Basic password security IT policies is False.

The default value in all other preconfigured IT policies is True.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 3.6
- BlackBerry® Enterprise Server version 4.0

### Exceptions

The BlackBerry® Enterprise Server for Novell® GroupWise® supports this IT policy rule in BlackBerry Device Software versions 4.0 and later.

## Force Smart Card Two Factor Authentication IT policy rule

### Description

This rule specifies whether a user must type a BlackBerry® device password and the smart card password to unlock a BlackBerry device.

### Default value

The default value is False.

### Usage

If you change this rule to True, to unlock a BlackBerry device, a user might require an authenticator module for a smart card and must have a smart card driver and a BlackBerry® Smart Card Reader driver installed on the BlackBerry device.

### Dependencies

If you change this rule to True, the BlackBerry® Enterprise Server automatically configures the Password Required IT policy rule to True in the same IT policy. You must configure the Password Required IT policy rule to True manually for a BlackBerry device that is running BlackBerry® Device Software versions 4.2 and earlier.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0
- BlackBerry Device Software version 3.6
- BlackBerry Smart Card Reader software version 1.5
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® and BlackBerry® Enterprise Server for Novell® GroupWise® version 4.0
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.6

### Exceptions

The BlackBerry Enterprise Server for Novell GroupWise supports this rule in BlackBerry Device Software version 4.0 or later.

## Force Smart Card Two Factor Challenge Response IT policy rule

### Description

This rule specifies whether the 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.

### Default value

The default value is False.

### Usage

If you change this rule to True, when the user unlocks a BlackBerry device, the BlackBerry device sends a challenge to the smart card to verify the authenticator module for the smart card.

If you change this rule to True, to use a BlackBerry device, a user must have a BlackBerry® Smart Card Reader, and must install a smart card driver and a BlackBerry Smart Card Reader driver on the BlackBerry device.

### Dependencies

A BlackBerry device uses this rule only if you configure the Password Required and Force Smart Card Two Factor Authentication IT policy rules to True.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 4.2
- BlackBerry Smart Card Reader software version 1.5
- BlackBerry® Enterprise Server version 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 cached password timeout expires in the key store. After the timeout expires, a BlackBerry® device prompts the user to type the password. The permitted range is 1 through 60 minutes.

**Default value**

The default value is 1 minute.

**Usage**

If you change this rule to 0, a BlackBerry device cannot cache the key store password and cannot reduce the number of password prompts.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 3.6
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® and BlackBerry® Enterprise Server for Novell® GroupWise® version 4.0
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.6

**Exceptions**

The BlackBerry Enterprise Server for Novell GroupWise supports this rule in BlackBerry Device Software version 4.0 or later.

## Lock on Smart Card Removal IT policy rule

**Description**

This rule specifies whether a BlackBerry® device locks when the user removes the paired smart card from the BlackBerry® Smart Card Reader or disconnects the BlackBerry Smart Card Reader from a BlackBerry device.

Not all smart card reader drivers support smart card removal detection.

**Default value**

The default value is False.

**Usage**

If you change this rule to True, to use a BlackBerry device, users might require an authenticator module for the smart card and must have a smart card driver and a BlackBerry Smart Card Reader driver installed on the BlackBerry device.

**Dependencies**

If you change this rule to True, the BlackBerry® Enterprise Server configures the Password Required and Force Smart Card Two Factor Authentication IT policy rules to True automatically in the same IT policy.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 3.6
- BlackBerry® Enterprise Server for IBM® Lotus® Domino® and Novell® GroupWise® version 4.0
- BlackBerry® Enterprise Server for Microsoft® Exchange version 3.6

**Exceptions**

The BlackBerry Enterprise Server for Novell GroupWise supports this rule in BlackBerry Device Software version 4.0 or later.

## 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. Each period, the BlackBerry device requests the status of the certificate. If the certificate is revoked, the BlackBerry device locks and the user is unable to unlock it unless the certificate status changes from On Hold to Good. The permitted range between status checks is 240 to 40320 minutes.

**Default value**

The default value is -1, which specifies no time limit.

**Dependencies**

A BlackBerry device uses this rule only if you configure the Password Required, Force Smart Card User Authentication, and Force Smart Card Two Factor Challenge Response IT policy rules to True.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.5
- BlackBerry® Enterprise Server version 4.1 SP5

## Message Classification IT policy rule

### Description

This rule specifies the set of message classifications that are available to apply to email messages sent using the BlackBerry® Enterprise Server.

### Default value

The default value is a null value.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 4.2
- BlackBerry Enterprise Server version 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 users apply the message classification to email messages.

### Default value

The default value is a null value.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.3
- BlackBerry® Enterprise Server version 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.

### Default value

The default value is Low security. A BlackBerry device never prompts the user for the key store password when accessing the private key to encrypt messages.

### Usage

If you change this rule to Medium security, a BlackBerry device prompts the user for the key store password when accessing the private key to encrypt messages only if the password is cleared from the key store cache.

If you change this rule to High security, a BlackBerry device always prompts the user for the key store password when accessing the private key to encrypt messages. If the user typed the password recently, the BlackBerry device prompts the user to confirm the password.

When you configure this rule, all keys must use the security level that you configure as the minimum, but a user can configure a higher security level on the BlackBerry device.

#### **Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 4.0
- BlackBerry® Enterprise Server version 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.

### **Default value**

The default value is Low security. A BlackBerry device never prompts the user for the key store password when accessing the private key to sign messages.

### **Usage**

If you change this rule to Medium security, a BlackBerry device prompts the user for the key store password when accessing the private key to sign messages only if the password is cleared from the key store cache.

If you change this rule to High security, a BlackBerry device always prompts the user for the key store password when accessing the private key to sign messages. If the user typed the password recently, the BlackBerry device prompts the user to confirm the password.

When you configure this rule, keys must use the security level that you configure as the minimum, but the user can configure a higher security level on a BlackBerry device.

### **Minimum requirements**

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

## Password Required for Application Download IT policy rule

### Description

This rule specifies whether a BlackBerry® device prompts a user for the BlackBerry device password when using the browser to download applications.

### Default value

The default value is False.

### Dependencies

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

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.2.2
- BlackBerry® Enterprise Server version 4.1 SP4

## Required Password Pattern IT policy rule

### Description

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

Passwords can contain Latin-1 characters only.

### Default value

The default value is a null value.

### Usage

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

- a: Permits any letter.
- A: Permits an uppercase letter only.
- c: Permits any consonant 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.

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

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

#### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 4.2
- BlackBerry® Enterprise Server version 4.0 SP6

## Remote Wipe Reset to Factory Defaults IT policy rule

### Description

This rule specifies whether a BlackBerry® device resets to the default settings when it receives the Erase Data and Disable Handheld IT administration command over a wireless network.

### Default value

The default value is False.

### Usage

Change this rule to True to require a BlackBerry device to delete its stored IT policy permanently, to delete all third-party applications, and to delete all user data.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.2.2
- BlackBerry® Enterprise Server version 4.1 SP4

## Require Secure APB Messages IT policy rule

### Description

This rule specifies whether the BlackBerry® device can receive email messages that are not secure, including APB messages from a BlackBerry® Enterprise Server.

### Default value

The default value is False.

### Usage

A BlackBerry device can receive all email messages from the BlackBerry Enterprise Server that are not blocked at the BlackBerry device firewall unless you change this rule to True.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 4.2
- BlackBerry Enterprise Server version 4.0 SP6

## Secure Wipe Delay After IT Policy Received IT policy rule

### Description

This rule specifies the length of time (in hours) that can elapse after receiving an IT policy update that a BlackBerry® device deletes all user data. The permitted range is 2 through 720 hours.

### Default value

The default value is disabled.

### Usage

Use this rule to require that a BlackBerry device that cannot receive IT policy updates or IT administration commands delete user data after a specific period of time.

### Dependencies

If you configure this rule to prevent deleting user data unexpectedly, on the BlackBerry® Enterprise Server, in the IT Admin properties, configure the Policy Resend Interval to a lower value than the value that you configure in this rule.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 4.2
- BlackBerry Enterprise Server version 4.0 SP6

## Secure Wipe Delay After Lock IT policy rule

### Description

This rule specifies the length of time (in hours) that can elapse after a BlackBerry® device locks that the device deletes all user data. The permitted range is 2 through 720 hours.

### Default setting

The default setting is disabled.

### Usage

Use this rule to require that a BlackBerry device delete the user data if the user has not unlocked the BlackBerry device within the specified period of time.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 4.2
- BlackBerry® Enterprise Server version 4.0 SP6

## Secure Wipe if Low Battery IT policy rule

### Description

This rule specifies whether a BlackBerry® device deletes all user data if the battery power level is too low.

### Default value

The default value is False.

### Usage

Use this rule to require that a BlackBerry device that cannot receive IT policy updates or IT administration commands deletes user data when the battery power level is too low.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 4.2
- BlackBerry® Enterprise Server version 4.0 SP6

## Security Service Colors IT policy rule

### Description

This rule specifies two background colors 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 BlackBerry 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 BlackBerry device receives from other services (for example, from the BlackBerry® Internet Service).

### Default value

The default value is a null value.

### Usage

You might configure this rule to one of the following example colors:

- 0xffffffff: white
- 0x000000: black
- 0xff0000: red

- 0x00ff00: green
- 0x0000ff: blue

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 4.0
- BlackBerry Enterprise Server version 4.0

## Security Transcoder Cod File Hashes IT policy rule

**Description**

This rule specifies which .cod files a BlackBerry® device permits to register as transcoders.

**Attention:** If you specify third-party applications that can use the Transcoder API on a BlackBerry device, those applications might impact the security, usability, and performance of the BlackBerry® Enterprise Solution. For more information, see the *BlackBerry Enterprise Solution Security Technical Overview*.

**Default value**

The default value is a null value.

**Usage**

To permit a third-party encryption scheme to be used in conjunction with BlackBerry Enterprise Solution encryption, configure hashes in hexadecimal format, separated by commas. A BlackBerry device reads this information from the command `javaloader siblinginfo <implementation_file.cod>`.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.5
- BlackBerry® Enterprise Server version 4.1 SP5

## Trusted Certificate Thumbprints IT policy rule

**Description**

This rule specifies the Hex-ASCII certificate thumbprints used on a BlackBerry® device that are generated using the SHA-1 or MD5 algorithm. Separate multiple thumbprints with a semi-colon.

**Default value**

The default value is a null value.

**Usage**

If you configure this rule, a user can only add certificates to the trusted key store that use the thumbprints that appear in the defined list.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 3.6
- BlackBerry® Enterprise Server version 3.6

**Exceptions**

The BlackBerry® Enterprise Server for Novell® GroupWise® supports this rule in BlackBerry Device Software versions 4.0 and later.

## Weak Digest Algorithms IT policy rule

**Description**

This rule specifies the digest algorithms that a BlackBerry® device considers weak. When a BlackBerry device sends email messages, it uses the algorithms that it considers strong to digitally sign the messages. A BlackBerry device uses the list of weak digest algorithms to verify the following data:

- algorithms that are used to digitally sign messages that a BlackBerry device receives are strong enough
- certificate chains for the certificates that are used to sign messages that a BlackBerry device receives are strong enough

**Default value**

By default, no algorithms are specified as weak.

**Usage**

Specify a list of algorithms that a BlackBerry device considers weak. This prevents a user from sending an S/MIME-encrypted or PGP® encrypted message using a certificate or key that has a corresponding public key that is weak. You cannot specify SHA-384 and SHA-512 as weak algorithms.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.3
- BlackBerry® Enterprise Server version 4.1 SP5

## Service Exclusivity policy group

### Allow Other Browser Services IT policy rule

**Description**

This rule specifies whether a BlackBerry® device can use other browser services.

**Default value**

The default value is True.

**Usage**

Change this rule to False to require that a BlackBerry device send browser data through your organization's BlackBerry® Enterprise Server, and to prevent a user from installing other browser services on a BlackBerry device.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0 (internal)
- BlackBerry® Device Software version 3.6
- BlackBerry Enterprise Server version 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.

**Default value**

The default value is True.

**Usage**

Change this rule to False to require that a BlackBerry device user in your organization sends appointments using a BlackBerry® Enterprise Server within your organization's environment.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.3
- BlackBerry Enterprise Server version 4.1 SP5

## Allow Other Message Services IT policy rule

**Description**

This rule specifies whether a BlackBerry® device can use other email message services.

**Default value**

The default value is True.

### Usage

Change this rule to False to require that a BlackBerry device user send outgoing email messages through your organization's BlackBerry® Enterprise Server and to prevent a user from sending email messages using other email message services.

This rule does not prevent a user from receiving email messages on a BlackBerry device from other email message services.

### Minimum requirements

- C++ based BlackBerry device that is running BlackBerry® Device Software version 2.5
- Java® based BlackBerry device that is running BlackBerry Device Software version 3.6
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 2.1
- BlackBerry Enterprise Server version 3.5

## Allow Public AIM Services IT policy rule

### Description

This rule specifies whether a user can use AOL® Instant Messenger™ (AIM® service) on a BlackBerry® device.

### Default value

The default value is True.

### Usage

Change this rule to False to prevent communication using AIM on a BlackBerry device.

### Minimum requirements

- BlackBerry® Application Suite version 1.0
- BlackBerry® Enterprise Server version 3.6 SP6

## Allow Public Google Talk Services IT policy rule

### Description

This rule specifies whether a user can use Google Talk™ on a BlackBerry® device.

### Default value

The default value is True.

### Usage

Change this rule to False to prevent communication using Google Talk on a BlackBerry device.

If you change this rule to False and a user has downloaded the Google Talk for BlackBerry devices application, the Google Talk for BlackBerry device icon remains on the Home screen. If a user tries to sign into the application, a message appears indicating that they cannot use the application.

**Minimum requirements**

- BlackBerry® Application Suite version 1.0
- BlackBerry® Enterprise Server version 4.0 SP4

## Allow Public ICQ Services IT policy rule

**Description**

This rule specifies whether a user can use ICQ® on a BlackBerry® device.

**Default value**

The default value is True.

**Usage**

Change this rule to False to prevent communication using ICQ on a BlackBerry device.

**Minimum requirements**

- BlackBerry® Application Suite version 1.0
- BlackBerry® Enterprise Server version 3.6 SP6

## Allow Public IM Services IT policy rule

**Description**

This rule specifies whether a user can use public instant messaging applications for BlackBerry® devices.

**Default value**

The default value is True.

**Usage**

Change this rule to False to prevent using public instant messaging services on a BlackBerry device.

This rule applies to all Research In Motion® public instant messaging services for BlackBerry devices that were released after the first availability of this rule. To prevent a user from using Yahoo!® Messenger for BlackBerry® smartphones version 1.0 on a BlackBerry device, configure the Allow Public Yahoo! Messenger Services IT policy rule.

**Minimum requirements**

- BlackBerry® Application Suite version 1.0
- BlackBerry® Enterprise Server version 4.0 SP4

## Allow Public WLM Services IT policy rule

### Description

This rule specifies whether a user can use Windows Live™ Messenger on a BlackBerry® device.

### Default setting

The default value is True.

### Usage

Change this rule to False to prevent communication using Windows Live Messenger on a BlackBerry device.

### Minimum requirements

- BlackBerry® Enterprise Server version 4.1 SP5

## Allow Public Yahoo! Messenger Services IT policy rule

### Description

This rule specifies whether a user can use Yahoo!® Messenger on a BlackBerry® device.

### Default value

The default value is True.

### Usage

Change this rule to False to prevent communication using Yahoo! Messenger on a BlackBerry device.

### Minimum requirements

- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0
- BlackBerry® Enterprise Server version 3.6 SP4

## SIM Application Toolkit policy group

### 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 certain location-related information.

#### Default setting

The default setting is False.

### Usage

The information that the SIM card can query is limited to the current wireless network and cell identities, BlackBerry device IMEI, date, time, and some measurement results.

### Minimum requirements

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

### Default setting

The default setting is False.

### Minimum requirements

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

### Default setting

The default setting is False.

### Minimum requirements

- Java® based BlackBerry® device
- S/MIME Support Package for BlackBerry® smartphones version 4.0

- BlackBerry® Connect™ version 4.0
- BlackBerry® Application Suite version 1.0
- BlackBerry® Device Software version 3.6
- BlackBerry® Enterprise Server version 4.0 SP3

## Smart Dialing policy group

### Enable Smart Dialing Policy IT policy rule

#### Description

This rule specifies whether smart dialing for VoIP calls is available on a BlackBerry® device.

#### Default setting

The default setting is True.

#### Usage

This rule is obsolete in BlackBerry® Enterprise Server versions 4.1 SP4 and later and BlackBerry® Device Software versions 4.0.2 and later.

#### Minimum requirements

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

### Set Local Area Code IT policy rule

#### Description

This rule specifies the local area code for phone numbers.

#### Default value

The default value is a null value.

#### Usage

This rule is obsolete in BlackBerry® Enterprise Server versions 4.1 SP4 and later and BlackBerry® Device Software versions 4.0.2 and later.

#### Dependencies

A BlackBerry device uses this rule only if you configure the Enable Smart Dialing IT policy rule to True.

**Minimum requirements**

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

## Set Local Country Code IT policy rule

**Description**

This rule specifies the local country code for phone numbers.

**Default value**

The default value is a null value.

**Usage**

This rule is obsolete in BlackBerry® Enterprise Server versions 4.1 SP4 and later and BlackBerry® Device Software versions 4.0.2 and later.

**Dependencies**

A BlackBerry device uses this rule only if you configure the Enable Smart Dialing IT policy rule to True.

**Minimum requirements**

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

## Set National Number Length IT policy rule

**Description**

This rule specifies the national phone number length.

**Default value**

The default value is a null value.

**Usage**

This rule is obsolete in BlackBerry® Enterprise Server versions 4.1 SP4 and later and BlackBerry® Device Software versions 4.0.2 and later.

**Dependencies**

A BlackBerry device uses this rule only if you configure the Enable Smart Dialing IT policy rule to True.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry Device Software version 4.0
- BlackBerry Enterprise Server version 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.

**Default value**

The default value is True.

**Usage**

This rule is obsolete in BlackBerry® Enterprise Server versions 4.1 SP4 and later and BlackBerry® Device Software versions 4.2.2 and later.

**Dependencies**

A BlackBerry device uses this rule only if you configure the Enable Smart Dialing IT policy rule to True.

**Minimum requirements**

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

## TCP policy group

### TCP APN IT policy rule

**Description**

This rule specifies whether a default APN is required when a BlackBerry® device uses TCP. The length of this string is limited to 120 characters.

**Default value**

The default value is a null value.

**Minimum requirements**

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

## TCP Password IT policy rule

### Description

This rule specifies whether a default APN password must be used when a BlackBerry® device uses TCP. The length of this string is limited to 32 characters.

### Default value

The default value is a null value.

### Minimum requirements

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

## TCP Username IT policy rule

### Description

This rule specifies whether a default APN user name is required when a BlackBerry® device uses TCP. The length of this string is limited to 32 characters.

### Default value

The default value is a null value.

### Minimum requirements

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

## TLS policy group

### TLS Device Side Only IT policy rule

#### Description

This rule specifies whether a BlackBerry® device and the BlackBerry® Enterprise Server can use proxy mode TLS or proxy mode HTTPS.

#### Default value

The default value is False.

#### Usage

If you change this rule to True, all HTTPS connections must use TLS on the device.

If you change this rule and TLS is not available on the BlackBerry device, an exception occurs.

#### Minimum requirements

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

### TLS Disable 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.

#### Default value

The default value is Prompt user on BlackBerry device.

#### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 3.6.1
- BlackBerry® Enterprise Server version 3.6

## TLS Disable Untrusted Connection IT policy rule

### Description

This rule specifies whether to prevent a BlackBerry® device from permitting TLS connections to untrusted servers.

### Default value

The default value is Prompt user on BlackBerry device.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 3.6.1
- BlackBerry® Enterprise Server version 3.6

## TLS Disable Weak Ciphers IT policy rule

### Description

This rule specifies whether to prevent a BlackBerry® device from using weak algorithms over TLS connections.

### Default value

The default value is Prompt user on BlackBerry device.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 3.6.1
- BlackBerry® Enterprise Server version 3.6

## TLS Minimum Strong DH Key Length IT policy rule

### Description

This rule specifies the minimum DH key size (in bits) to use over TLS connections. The permitted range is 512 through 4096 bits.

### Default value

The default value on a BlackBerry® device is 1024 bits.

The default value on the BlackBerry® Enterprise Server is 512 bits.

### Usage

If you configure the minimum key size on the BlackBerry Enterprise Server to be higher than the minimum key size on a BlackBerry device, the BlackBerry device continues to prompt the user to trust every secure web site that uses a key size in its certificate that is less than the minimum key size on the BlackBerry Enterprise Server.

For example, when a user browses to a secure web site that uses a 512-bit DH key in its certificate, the BlackBerry device prompts the user to trust the web site. If the user trusts the web site and selects the Don't Ask Again option, the minimum key size on the BlackBerry device is configured to 512 bits. If you set the minimum key size on the BlackBerry Enterprise Server to 2048 bits, the BlackBerry device continues to prompt the user to trust every secure web site that uses a key size in its certificate that is less than 2048 bits.

#### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 3.6.1
- BlackBerry Enterprise Server version 3.6

## TLS Minimum Strong DSA Key Length IT policy rule

### Description

This rule specifies the minimum DSA key size (in bits) to use over TLS connections. The permitted range is 512 through 1024 bits.

### Default value

The default value on a BlackBerry® device is 1024 bits.

The default value on the BlackBerry® Enterprise Server is 512 bits.

### Usage

If you configure the minimum key size on the BlackBerry Enterprise Server to be higher than the minimum key size on the BlackBerry device, the BlackBerry device continues to prompt the user to trust every secure web site that uses a key size in its certificate that is less than the minimum key size on the BlackBerry Enterprise Server.

For example, when a user browses to a secure web site that uses a 512-bit DSA key in its certificate, the BlackBerry device prompts the user to trust the web site. If the user trusts the web site and selects the Don't Ask Again option, the minimum key size on the BlackBerry device is configured to 512 bits. If you configure the minimum key size on the BlackBerry Enterprise Server to 1024 bits, the BlackBerry device continues to prompt the user to trust every secure web site that uses a key size in its certificate that is less than 1024 bits.

#### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 3.6.1
- BlackBerry Enterprise Server version 3.6 SP1

## TLS Minimum Strong ECC Key Length IT policy rule

### Description

This rule specifies the minimum ECC key size (in bits) to use over TLS connections. The permitted range is 160 through 571 bits.

### Default value

The default value on a BlackBerry® device is 163 bits.

The default value on the BlackBerry® Enterprise Server is 160 bits.

### Usage

If you configure the minimum key size on the BlackBerry Enterprise Server to be higher than the minimum key size on the BlackBerry device, the BlackBerry device continues to prompt the user to trust every secure web site that uses a key size in its certificate that is less than the minimum key size on the BlackBerry Enterprise Server.

For example, when a user browses to a secure web site that uses a 160-bit ECC key in its certificate, the BlackBerry device prompts the user to trust the web site. If the user trusts the web site and selects the Don't Ask Again option, the minimum key size on the BlackBerry device is configured to 160 bits. If you configure the minimum key size on the BlackBerry Enterprise Server to 233 bits, the BlackBerry device continues to prompt the user to trust every secure web site that uses a key size in its certificate that is less than 233 bits.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 3.6.1
- BlackBerry Enterprise Server version 3.6

## TLS Minimum Strong RSA Key Length IT policy rule

### Description

This rule specifies the minimum RSA® key size (in bits) to use over TLS connections. The permitted range is 512 through 4096 bits.

### Default value

The default value on the BlackBerry® device is 1000 bits.

The default value on the BlackBerry® Enterprise Server is 512 bits.

### Usage

If you configure the minimum key size on the BlackBerry Enterprise Server to be higher than the minimum key size on the BlackBerry device, the BlackBerry device continues to prompt the user to trust every secure web site that uses a key size in its certificate that is less than the minimum key size on the BlackBerry Enterprise Server.

For example, when a user browses to a secure web site that uses a 512-bit RSA key in its certificate, the BlackBerry device prompts the user to trust the web site. If the user trusts the web site and selects the Don't Ask Again option, the minimum key size on the BlackBerry device is configured to 512 bits. If you configure the minimum key size on the BlackBerry Enterprise Server to 2048 bits, the BlackBerry device continues to prompt the user to trust every secure web site that uses a key size in its certificate that is less than 2048 bits.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 3.6.1
- BlackBerry Enterprise Server version 3.6

## TLS Restrict FIPS Ciphers IT policy rule

**Description**

This rule specifies whether a BlackBerry® device can use an algorithm with TLS that is not FIPS-compliant.

**Default value**

The default value is False.

**Usage**

By default, if you configure the FIPS Level IT policy rule to Level 2, a BlackBerry device does not use this rule and uses only algorithms that are FIPS-compliant.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 3.6.1
- BlackBerry® Enterprise Server version 3.6

## 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 to the BlackBerry® Device Software over the wireless network.

**Default value**

The default value is False.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry Device Software version 4.5
- BlackBerry® Enterprise Server version 4.1 SP4

## 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 a previously successful update of the BlackBerry Device Software over the wireless network.

**Default value**

The default value is False.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry Device Software version 4.5
- BlackBerry® Enterprise Server version 4.1 SP4

## Disallow Device User Requested Upgrade

**Description**

This rule specifies whether to prevent a BlackBerry® device user from requesting available updates for the BlackBerry® Device Software over the wireless network.

**Default value**

The default value is False.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry Device Software version 4.5
- BlackBerry® Enterprise Server version 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.

**Default value**

The default value is False.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry Device Software version 4.5
- BlackBerry® Enterprise Server version 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.

**Default value**

The default value is False.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry Device Software version 4.5
- BlackBerry® Enterprise Server version 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.

**Default value**

The default value is False.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry Device Software version 4.5
- BlackBerry® Enterprise Server version 4.1 SP4

## Disallow Patch Download Over WiFi 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.

### Default value

The default value is False.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry Device Software version 4.5
- BlackBerry® Enterprise Server version 4.1 SP4

## WTLS policy group

### WTLS Disable Invalid Connection IT policy rule

#### Description

This rule specifies whether to prevent a BlackBerry® device from permitting WTLS connections to servers that have invalid certificates.

#### Default value

The default value is Prompt user on BlackBerry device.

#### Usage

Change this rule to Disable invalid connections.

Change this rule to Allow invalid connections.

#### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 3.6
- BlackBerry® Enterprise Server version 3.6

### WTLS Disable Untrusted Connection IT policy rule

#### Description

This rule specifies whether to prevent a BlackBerry® device from permitting WTLS connections to untrusted servers.

**Default value**

The default value is Prompt user on BlackBerry device.

**Usage**

Change this rule to Disable untrusted connections.

Change this rule to Allow untrusted connections.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 3.6
- BlackBerry® Enterprise Server version 3.6

## WTLS Disable Weak Ciphers IT policy rule

**Description**

This rule specifies whether to prevent a BlackBerry® device from using weak algorithms over WTLS connections.

**Default value**

The default value is Prompt user on BlackBerry device.

**Usage**

Change this rule to Disable weak algorithms.

Change this rule to Allow weak algorithms.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 3.6
- BlackBerry® Enterprise Server version 3.6

## WTLS Minimum Strong DH Key Length IT policy rule

**Description**

This rule specifies the minimum DH key size (in bits) to use over WTLS connections. The permitted range is 512 through 4096 bits.

**Default value**

The default value on a BlackBerry® device is 1024 bits.

The default value on the BlackBerry® Enterprise Server is 512 bits.

### Usage

If you configure the minimum key size on the BlackBerry Enterprise Server to be higher than the minimum key size on a BlackBerry device, the BlackBerry device continues to prompt the user to trust every secure web site that uses a key size in its certificate that is lower than the minimum key size on the BlackBerry Enterprise Server.

For example, when a user browses to a secure web site that uses a 512-bit DH key in its certificate, the BlackBerry device prompts the user to trust the web site. If the user trusts the web site and selects the Don't Ask Again option, the minimum key size on the BlackBerry device is configured to 512 bits. If you configure the minimum key size on the BlackBerry Enterprise Server to 2048 bits, the BlackBerry device continues to prompt the user to trust every secure web site that uses a key size in its certificate that is lower than 2048 bits.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 3.6
- BlackBerry Enterprise Server version 3.6

## WTLS Minimum Strong ECC Key Length IT policy rule

### Description

This rule specifies the minimum ECC key size (in bits) to use over WTLS connections. The permitted range is 160 through 571 bits.

### Default value

The default value on the BlackBerry® device is 163 bits.

The default value on the BlackBerry® Enterprise Server is 160 bits.

### Usage

If you configure the minimum key size on the BlackBerry Enterprise Server to be higher than the minimum key size on a BlackBerry device, the BlackBerry device continues to prompt the user to trust every secure web site that uses a key size in its certificate that is lower than the minimum key size on the BlackBerry Enterprise Server.

For example, when a user browses to a secure web site that uses a 160-bit ECC key in its certificate, the BlackBerry device prompts the user to trust the web site. If the user trusts the web site and selects the Don't Ask Again option, the minimum key size on the BlackBerry device is configured to 160 bits. If you configure the minimum key size on the BlackBerry Enterprise Server to 233 bits, the BlackBerry device continues to prompt the user to trust every secure web site that uses a key size in its certificate that is lower than 233 bits.

### Minimum requirements

- Java® based BlackBerry device

- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 3.6
- BlackBerry Enterprise Server version 3.6

## WTLS Minimum Strong RSA Key Length IT policy rule

### Description

This rule specifies the minimum RSA® key size (in bits) to use over WTLS connections. The permitted range is 512 through 4096 bits.

### Default value

The default value on the BlackBerry® device is 1000 bits.

The default value on the BlackBerry® Enterprise Server is 512 bits.

### Usage

If you configure the minimum key size on the BlackBerry Enterprise Server to be higher than the minimum key size on a BlackBerry device, the BlackBerry device continues to prompt the user to trust every secure web site that uses a key size in its certificate that is lower than the minimum key size on the BlackBerry Enterprise Server.

For example, when a user browses to a secure web site that uses a 512-bit RSA key in its certificate, the BlackBerry device prompts the user to trust the web site. If the user trusts the web site and selects the Don't Ask Again option, the minimum key size on the BlackBerry device is configured to 512 bits. If you configure the minimum key size on the BlackBerry Enterprise Server to 2048 bits, the BlackBerry device continues to prompt the user to trust every secure web site that uses a key size in its certificate that is lower than 2048 bits.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite version 1.0
- BlackBerry® Connect™ version 4.0
- BlackBerry® Device Software version 3.6
- BlackBerry Enterprise Server version 3.6

## WTLS Restrict FIPS Ciphers IT policy rule

### Description

This rule specifies whether the BlackBerry® device can use an algorithm with WTLS that is not FIPS-compliant.

### Default value

The default value is False.

### Usage

By default, if you configure the FIPS Level IT policy rule to 2, a BlackBerry device ignores this rule and uses only algorithms that are FIPS-compliant.

**Minimum requirements**

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

# Application control policy rules

## 3

## Understanding application control policies

The BlackBerry® Enterprise Server application control policy rules are designed to allow or prevent the installation of specific third-party applications on the BlackBerry device, and to limit the permissions of third-party applications that are installed on the BlackBerry device.

After you assign a software configuration to a BlackBerry device, you can set the BlackBerry Enterprise Server to send the software configuration to the BlackBerry device over the wireless network. The user can use the application loader tool of the BlackBerry® Desktop Manager to install or upgrade to the BlackBerry® Device Software in the software configuration.

To control or change the behavior of third-party applications on the BlackBerry device, you can set an application control policy and assign values to the application control policy rules. If a default application control policy does not exist, the user can change some application control settings on the BlackBerry device. If a default application control policy exists, the user cannot change the application control settings.

## Setting application control policy rules

You can assign application control policy rules to satisfy your organization's security policy requirements and to reflect the needs of the users who are assigned to that application control policy.

You can set a default application control policy that blocks third-party applications from running on a BlackBerry® device. If a user connects a BlackBerry device that has third-party applications installed to a BlackBerry® Enterprise Server, it does not allow the third-party applications to run.

You can also set application control policies and apply them to trusted third-party applications to create an allowed application list for specific application behavior.

If the default application control policy prevents all third-party applications from performing specific actions, you can also use an allowed application list to allow applications to perform those actions.

For more information about making BlackBerry® Device Software and third-party applications available to users, see the *BlackBerry Enterprise Server System Administration Guide*.

# Descriptions of application control policy rules

## 4

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

## Security Data application control policy rule

### Description

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

### Default setting

The default setting is Allowed.

### Dependencies

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

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software Version 4.0
- BlackBerry® Enterprise Server Version 4.0

## BlackBerry Device Keystore Medium Security application control policy rule

### Description

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

### Default setting

The default setting is Allowed.

### Dependencies

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

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software Version 4.0

- BlackBerry® Enterprise Server Version 4.0

## Bluetooth Serial Profile application control policy rule

### Description

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

### Default setting

The default setting is Allowed.

### Dependencies

If you set the Disable Serial Port Profile IT policy rule to True, this application control policy rule does not apply. The BlackBerry® device cannot use the Bluetooth SPP to establish a serial connection to a Bluetooth enabled device.

### Minimum requirements

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

## Browser Filter Domains application control policy rule

### Description

This rule specifies the list of domains for which an application can apply browser filters to web page content on the 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 setting

The default setting is a null value.

### Minimum requirements

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

## Browser Filters application control policy rule

### Description

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

**Default setting**

The default setting is Not Permitted

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software Version 4.0
- BlackBerry® Enterprise Server Version 4.0

## Device GPS application control policy rule

**Description**

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

**Default setting**

The default setting is Prompt User.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.0
- BlackBerry® Enterprise Server version 4.1 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 mandatory on the BlackBerry device or to prevent unspecified or untrusted applications from being installed on the BlackBerry device.

**Default setting**

The default setting is Optional.

**Minimum requirements**

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

## Event Injection application control policy rule

### Description

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

### Default setting

The default setting is Not Permitted.

### Minimum requirements

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

## External Domains application control policy rule

### Description

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

### Default setting

The default setting is a null value.

### Minimum requirements

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

## External Network Connections application control policy rule

### Description

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

### Default setting

The default setting is Prompt User.

### Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.0

- BlackBerry® Enterprise Server version 4.0

## Internal Domains application control policy rule

### Description

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

### Default setting

The default setting is a null value.

### Minimum requirements

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

## Internal Network Connections application control policy rule

### Description

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

### Default setting

The default setting is Prompt User.

### Minimum requirements

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

## Cross Application Communication application control policy rule

### Description

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

### Default setting

The default setting is Allowed.

**Minimum requirements**

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

## Local Connections application control policy rule

**Description**

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

**Default setting**

The default setting is Allowed.

**Minimum requirements**

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

## Message Access application control policy rule

**Description**

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

**Default setting**

The default setting is Allowed.

**Minimum requirements**

- Java® based BlackBerry device
- BlackBerry® Device Software Version 4.0
- BlackBerry® Enterprise Server Version 4.0

## Phone Access application control policy rule

**Description**

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

**Default setting**

The default setting is Prompt User.

**Minimum requirements**

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

## Organizer Data Access application control policy rule

**Description**

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

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

**Default setting**

The default setting is Allowed.

**Minimum requirements**

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

## Themes application control policy rule

**Description**

This rule specifies whether custom theme applications developed using the Plazmic® Content Developer's Kit can be used as themes on the BlackBerry® device.

**Default setting**

The default setting is Allowed.

**Minimum requirements**

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

## User Authenticator 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 the BlackBerry® device. Currently, only smart card drivers are supported.

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

### Default setting

The default setting is Allowed.

### Minimum requirements

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

# BlackBerry MDS Services policy rules

## 5

### Configuring how users access and use BlackBerry MDS Runtime Applications

You can create BlackBerry® MDS Integration Service device policies and assign them to users and user groups to control how users access and use BlackBerry® MDS Runtime Applications on their BlackBerry devices. Device policies define whether users can upgrade the BlackBerry MDS Runtime, and whether users can discover, install, and remove BlackBerry MDS Runtime Applications from their BlackBerry devices. You can also use device policies to define whether BlackBerry MDS Runtime Applications can access data and other applications on the BlackBerry devices, and to specify message queue limits for data that BlackBerry MDS Runtime Applications send and receive.

## Descriptions of BlackBerry MDS Services policy rules

### Allow Runtime Upgrade By User BlackBerry MDS Services rule

**Description**

This rule specifies whether users can upgrade the BlackBerry® MDS Runtime on their BlackBerry devices.

**Default setting**

The default setting is False.

**Minimum requirements**

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

### Allow Discovery by User BlackBerry MDS Services rule

**Description**

This rule specifies whether users can search a BlackBerry® MDS Studio Application Repository for BlackBerry MDS Studio Applications that can be installed on their BlackBerry devices.

**Default setting**

The default setting is True.

**Minimum requirements**

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

### Allow Application Install by User BlackBerry MDS Services rule

**Description**

This rule specifies whether users can install BlackBerry® MDS Studio Applications on their BlackBerry devices.

**Default setting**

The default setting is 2.

**Usage**

Set this rule to 0 to prevent users from installing BlackBerry MDS Studio Applications.

Set this rule to 2 to permit users to install BlackBerry MDS Studio Applications.

**Minimum requirements**

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

## Allow Push Application Install BlackBerry MDS Services rule

**Description**

This rule specifies whether the BlackBerry® Enterprise Server administrator can send BlackBerry® MDS Studio Applications to the BlackBerry device.

**Default setting**

The default setting is True.

**Minimum requirements**

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

## Allow Application Delete by User BlackBerry MDS Services rule

**Description**

This rule specifies whether users can delete BlackBerry® MDS Studio Applications from their BlackBerry devices.

**Default setting**

The default setting is True.

**Minimum requirements**

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

## Allow External Access BlackBerry MDS Services rule

**Description**

This rule specifies whether BlackBerry® MDS Studio Applications that are installed on the BlackBerry device can access other applications and data, such as email messages and calendar entries.

**Default setting**

The default setting is 0.

**Usage**

Set this rule to 0 to prevent BlackBerry MDS Studio Applications from accessing data from other applications on the BlackBerry device.

Set this rule to 1 to permit BlackBerry MDS Studio Applications to retrieve data from other applications on the BlackBerry device.

Set this rule to 2 to permit BlackBerry MDS Studio Applications to retrieve data from and send data to other applications on the BlackBerry device.

**Minimum requirements**

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

## Allow Access to Multiple Domains BlackBerry MDS Services rule

**Description**

This rule specifies whether BlackBerry® MDS Studio Applications that are installed on the BlackBerry device can access web services in multiple domains.

**Default setting**

The default setting is False.

**Minimum requirements**

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

## Queue Limit for Inbound Application Messages BlackBerry MDS Services rule

**Description**

This rule specifies the maximum number of messages from BlackBerry® MDS Studio Applications that can be queued locally on the BlackBerry device. The permitted range is 1 through 50 messages.

**Default setting**

The default setting is 8 messages.

**Minimum requirements**

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

## Queue Limit for Outbound Application Messages BlackBerry MDS Services rule

**Description**

This rule specifies the maximum number of messages to BlackBerry® MDS Studio Applications that can be queued locally on the BlackBerry device. The permitted range is 1 through 50 messages.

**Default setting**

The default setting is 16 messages.

**Minimum requirements**

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

## Examples of security policy goals

7

You can use IT policies and application control policies to meet your organization's security policy goals.

Example goal	Description
Define permitted use of passwords for authentication on BlackBerry® devices.	<ul style="list-style-type: none"> <li>• Require a password on the BlackBerry device.</li> <li>• Configure features such as password duration, length, and strength.</li> <li>• Require password patterns.</li> <li>• Forbid specific passwords.</li> </ul>
Define the encryption strength that BlackBerry devices use to protect data.	<ul style="list-style-type: none"> <li>• Extend encryption of data that is in transit between the sender and recipient of an email message or PIN message.</li> <li>• Require the BlackBerry device to generate and use the content protection key to encrypt user data while the BlackBerry device is locked.</li> <li>• Require the BlackBerry device to generate and use the grand master key to encrypt the master encryption key while the BlackBerry device is locked.</li> <li>• To require a specific standard of encryption strength, specify the level of FIPS compliance for the embedded cryptographic module that is required for basic operation of the BlackBerry device.</li> </ul>
Control application installation and use on BlackBerry devices.	<ul style="list-style-type: none"> <li>• Prevent BlackBerry device users from downloading third-party applications over the wireless network.</li> <li>• Specify whether applications on the BlackBerry device can establish specific types of connections.</li> </ul>
Block viruses and malicious user actions on BlackBerry devices.	<ul style="list-style-type: none"> <li>• Specify the resources (for example, email, phone, and BlackBerry device key store) that a third-party application can access on the BlackBerry device.</li> <li>• Specify the types of connections (for example, local, internal, and external) that a third-party application that is running on the BlackBerry device can open.</li> <li>• Specify whether an application can access the user authenticator framework API, which permits the registration of drivers to provide two-factor authentication to unlock the BlackBerry device.</li> </ul>
Control Bluetooth® technology use on BlackBerry devices.	<ul style="list-style-type: none"> <li>• Manage Bluetooth technology on BlackBerry devices.</li> <li>• Prevent the use of Bluetooth technology on BlackBerry devices.</li> </ul>

Example goal	Description
	<ul style="list-style-type: none"> <li>Specify whether a BlackBerry device can pair with another Bluetooth enabled device.</li> <li>Specify whether the user can turn on and turn off the Bluetooth profiles that are on the BlackBerry device.</li> </ul>

## Defining acceptable use of passwords and passphrases on BlackBerry devices

Scenario	Example IT policy rule	Example value
Extend your organization's password policy to BlackBerry® devices.	Password Required	True
	Maximum Password Age	30 (days)
	Minimum Password Length	8 (characters)
	Password Pattern Checks	2 (requires at least one alphabetic, one numeric, and one special character)
	Forbidden Passwords	obvious and non-secure passwords (for example, "password," usernames, and organization's names)
	Set Password Timeout	5 (minutes)
Delete all user data on the BlackBerry device if the user types the password incorrectly.	User Can Change Timeout	False
	Set Maximum Password Attempts	10 (number of incorrect passwords that a user types before the BlackBerry device data is deleted)
Do not permit users to reuse an expired password.	Maximum Password History	10 (maximum number of previous passwords that the new password must be checked against)
Permit users to notify administrators if the BlackBerry device is in jeopardy of theft.	Duress Notification Address	email address that receives a notification message when a user types a password under duress

## Defining measures to protect BlackBerry devices from unauthorized use

Scenario	Example IT policy rule	Example value
Extend your organization's password policy to BlackBerry® devices.	Enable Long Term Timeout	True
Lock the BlackBerry device automatically, regardless of user activity.		
Prompt the user to type a password, whether the BlackBerry device is idle or in use.	Periodic Challenge Time	60 (minutes that can elapse before the user must type a password)
Lock the BlackBerry device automatically when a user inserts it in the holster.	Force Lock When Holstered	True
Lock the BlackBerry device automatically after a period of user inactivity.	Maximum Security Timeout	5 (minutes of idle time that is permitted before the BlackBerry device locks)

## Defining the encryption strength that the BlackBerry device uses to protect data

Scenario	Example IT policy rule	Example value
Protect user and application data on the BlackBerry® device.	Content Protection Strength	True
Protect the master encryption key on a locked BlackBerry device.	Force Content Protection of Master	True
Specify the level of FIPS compliance on the BlackBerry device.	FIPS Level	2
Specify the algorithms that the BlackBerry device uses to encrypt and decrypt PGP® messages.	PGP Allowed Content Ciphers	AES (256-bit), AES (192-bit), AES (128-bit), and Triple DES

Scenario	Example IT policy rule	Example value
Specify the algorithms that the BlackBerry device uses to encrypt and decrypt S/MIME messages.	S/MIME Allowed Content Ciphers	AES (256-bit), AES (192-bit), AES (128-bit), and Triple DES

## Restricting unsecured messaging

Scenario	Example IT policy rule	Example value
To comply with industry regulations, make sure that all electronic communication between your employees and their clients is recorded.	Allow Other Browser Services	False
	Allow Other Message Services	False
	Allow Peer-to-Peer Messages	False
	Allow SMS	False
	Disable Forwarding Between Services	True
	Disable Cut/Copy/Paste	True
Prevent users from sending PIN messages. (Users can still receive PIN messages.)	Allow Peer-to-Peer Messages	False
Prevent users from sending SMS text messages. (Users can still receive SMS text messages.)	Allow SMS	False
Prevent users from forwarding or replying to messages using a different BlackBerry® Enterprise Server.	Disable Forwarding Between Services	True
Display message sensitivity using different message background colors.	Security Service Colors	colors of sensitive and nonsensitive messages in red-green-blue format

## Defining measures to prevent threats from viruses and malicious users

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

## Limiting the resources that third-party applications installed on BlackBerry devices can access

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

## Limiting user control of third-party applications on BlackBerry devices

Scenario	Example policy rule	Value
Prevent third-party applications from accessing serial ports or USB ports on BlackBerry® devices.	Allow Third Party Apps to Use Serial Port (IT policy rule)	False
Prevent third-party applications from accessing the persistent store API on BlackBerry devices.	Allow Third Party Apps to Use Persistent Store (IT policy rule)	False
Prevent users from configuring and running add-in applications in the BlackBerry® Desktop Manager.	Set Desktop Allow Desktop Add-Ins (IT policy rule)	False
Prevent users from downloading third-party applications or themes to their BlackBerry devices.	Disallow Third Party Application Downloads (IT policy rule)	True
Prevent users from removing a third-party Java® application installed on their BlackBerry devices.	Disposition (application control policy rule)	Required
Prevent users from installing a third-party Java application on their BlackBerry devices.	Disposition (application control policy rule)	Required
Remove a third-party Java application from BlackBerry devices over the wireless network.	Disposition (application control policy rule)	Required
Prevent users from turning on a custom theme that was created using the Plazmic® Content Developer's Kit.	Themes (application control policy rule)	Required
Prevent users from unlocking their BlackBerry devices using a BlackBerry® Smart Card Reader and an authentication password.	User Authenticator (application control policy rule)	Required
Prevent users that are authenticating through a VPN connection from using third-party applications on their BlackBerry devices.	User Authenticator (application control policy rule)	Required

## Preventing RIM value-added applications from running on BlackBerry devices

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

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

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

Application	Method
BlackBerry Wallet	<ul style="list-style-type: none"> <li>• Configure the Disable BlackBerry Wallet IT policy rule to True.</li> <li>• Apply an application control policy rule to block all third-party applications, or apply an application control policy to block specific RIM value-added applications if you want to remove the RIM value-added applications from BlackBerry devices.</li> <li>• Configure the Disable RIM Value-Added Applications IT policy rule to True.</li> </ul>
ecommerce content optimization engine for the BlackBerry Browser	<ul style="list-style-type: none"> <li>• Configure the Disable Ecommerce Content Optimization Engine IT policy rule to True.</li> <li>• Apply an application control policy rule to block all third-party applications, or apply an application control policy to block specific RIM value-added applications if you want to remove the RIM value-added applications from BlackBerry devices.</li> <li>• Configure the Disable RIM Value-Added Applications IT policy rule to True.</li> </ul>
BlackBerry Client for IBM Lotus Connections	<ul style="list-style-type: none"> <li>• Configure the Disable Lotus Connections IT policy rule to True.</li> <li>• Apply an application control policy rule to block all third-party applications, or apply an application control policy to block specific RIM value-added applications if you want to remove the RIM value-added applications from BlackBerry devices.</li> <li>• Configure the Disable RIM Value-Added Applications IT policy rule to True.</li> </ul>

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

## Example application control policies

### Blocking all third-party applications

When the Disallow Third Party Application Download IT policy rule is set to True, it prevents BlackBerry® devices from downloading third-party applications over the wireless network. It does not remove existing third-party applications from the BlackBerry devices. You can set a default application control policy to block all third-party applications from running on a BlackBerry device.

When you assign the application control policy to the user, the third-party applications exist on the BlackBerry device, but they cannot run. If the user tries to install additional third-party applications, the installation is unsuccessful and the BlackBerry device displays an authorization failure message.

### Block all third-party applications

1. In the BlackBerry® Manager, on the **Software Configuration** screen, click **Manage Application Policies**.
2. Create and name an application control policy.
3. To remove all existing third-party applications from the BlackBerry device and prevent the BlackBerry device from installing any new third-party applications, set **Disposition** to **Disallowed**.
4. Select a software configuration.
5. Click **Edit Configuration**.
6. Apply the application control policy to the default third-party applications for all BlackBerry devices, or to a specific BlackBerry device series.
7. Click **OK**.

### Permitting specific third-party applications

You can use a default application control policy that blocks all third-party applications.

To permit specific third-party applications to run on BlackBerry® devices, you can register those applications in the shared folder and apply a new application control policy that permits only those applications. When users try to download third-party applications to their BlackBerry devices, the devices add only the allowed applications.

To prevent users from deleting permitted third-party applications from their BlackBerry devices, you must set the application control policy to permit the application as required, instead of optional.

## Permit a specific third-party application while blocking all other third-party applications

You can use a default application control policy to block all third-party applications.

1. In the BlackBerry® Manager, on the **Software Configuration** screen, click **Edit Configuration**.
2. Click **Manage Application Policies**.
3. Create and name an application control policy.
4. To delete all existing third-party applications from the BlackBerry device and prevent the BlackBerry device from adding any new third-party applications, set **Disposition** to **Disallowed**.
5. To permit the third-party application, perform one of the following actions:
  - To permit the user to add the third-party application to the BlackBerry device, and to permit the user to delete the application from the BlackBerry device, set **Disposition** to **Optional**.
  - To push the application to the BlackBerry device over the wireless network automatically, and to prevent the user from deleting the application from the BlackBerry device, set **Disposition** to **Required**. In the software configuration, set the **Delivery** method to **Wireless**.
6. Apply the new application control policy to the third-party application.

## Controlling the behavior of third-party applications

To block specific threats to application security without banning all third-party applications on BlackBerry® devices, you can replace a default application control policy that blocks all third-party applications with a less restrictive application control policy that controls the behavior of third-party applications. You can allow specific behavior for registered third-party applications while preventing other third-party applications from exchanging data. By default, users can install other third-party applications but those other applications are not permitted to do anything on the BlackBerry devices.

## Assign a default application control policy to control the behavior of allowed third-party applications

You can restrict all available behavior for third-party applications. Applications that do not require access to the Internet, intranet, or BlackBerry® device data (for example, card games or calculators) can run on the BlackBerry device with all behavior restricted.

1. In the BlackBerry® Manager, on the **Software Configuration** screen, click **Edit Configuration**.
2. Click **Manage Application Policies**.
3. Create and name an application control policy.
4. To allow the user to install registered third-party applications on the BlackBerry device, set **Disposition** to **Optional**.
5. Assign the application control policy as the default application control policy.

## Legal notice

8

©2009 Research In Motion Limited. All rights reserved. BlackBerry®, RIM®, Research In Motion®, SureType®, SurePress™ and related trademarks, names, and logos are the property of Research In Motion Limited and are registered and/or used in the U.S. and countries around the world.

AIM, AOL, AOL Instant Messenger, and ICQ are trademarks of AOL LCC. Bluetooth is a trademark of Bluetooth SIG. DataViz is a trademark of Dataviz. IBM, Domino, Lotus, and Lotus Notes are trademarks of International Business Machines Corporation. Entrust and Entrust Entelligence are trademarks of Entrust, Inc. Facebook is a trademark of Facebook, Inc. Google Talk is a trademark of Google Inc. Microsoft, Windows, Windows Live, and Windows Live Messenger are trademarks of Microsoft Corporation. Novell and GroupWise are trademarks of Novell, Inc. PGP is a trademark of PGP Corporation. Plazmic Content Developer's Kit is a trademark of Plazmic Inc. Java and JavaScript are trademarks of Sun Microsystems, Inc. Wi-Fi is a trademark of the Wi-Fi Alliance. Yahoo! Messenger is a trademark of Yahoo! Inc. All other trademarks are the property of their respective owners.

The BlackBerry smartphone and other devices and/or associated software are protected by copyright, international treaties, and various patents, including one or more of the following U.S. patents: 6,278,442; 6,271,605; 6,219,694; 6,075,470; 6,073,318; D445,428; D433,460; D416,256. Other patents are registered or pending in the U.S. and in various countries around the world. Visit [www.rim.com/patents](http://www.rim.com/patents) for a list of RIM (as hereinafter defined) patents.

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

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

EXCEPT TO THE EXTENT SPECIFICALLY PROHIBITED BY APPLICABLE LAW IN YOUR JURISDICTION, ALL CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS, OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS OR WARRANTIES OF DURABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE, MERCHANTABILITY, MERCHANTABLE 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 RIM BE LIABLE FOR ANY TYPE OF DAMAGES RELATED TO THIS DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN INCLUDING WITHOUT LIMITATION ANY OF THE FOLLOWING DAMAGES: DIRECT, CONSEQUENTIAL, EXEMPLARY, INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, OR AGGRAVATED DAMAGES, DAMAGES FOR LOSS OF PROFITS OR REVENUES, FAILURE TO REALIZE ANY EXPECTED SAVINGS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, LOSS OF BUSINESS OPPORTUNITY, OR CORRUPTION OR LOSS OF DATA, FAILURES TO TRANSMIT OR RECEIVE ANY DATA, PROBLEMS ASSOCIATED WITH ANY APPLICATIONS USED IN CONJUNCTION WITH RIM PRODUCTS OR SERVICES, DOWNTIME COSTS, LOSS OF THE USE OF RIM PRODUCTS OR SERVICES OR ANY PORTION THEREOF OR OF ANY AIRTIME SERVICES, COST OF SUBSTITUTE GOODS, COSTS OF COVER, FACILITIES OR SERVICES, COST OF CAPITAL, OR OTHER SIMILAR PECUNIARY LOSSES, WHETHER OR NOT SUCH DAMAGES WERE FORESEEN OR UNFORESEEN, AND EVEN IF RIM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

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

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

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

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

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

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

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

Published in Canada