

BlackBerry Business Cloud Services

Policy Reference Guide



Contents

1	IT policy rules.....	5
	Preconfigured IT policies.....	5
	Default values for preconfigured IT policies.....	5
2	Descriptions of IT policy rules.....	7
	Device Only policy group.....	7
	Enable Long-Term Timeout IT policy rule.....	7
	Maximum Password Age IT policy rule.....	7
	Maximum Security Timeout IT policy rule.....	7
	Minimum Password Length IT policy rule.....	8
	Password Pattern Checks IT policy rule.....	8
	Password Required IT policy rule.....	9
	User Can Change Timeout IT policy rule.....	9
	User Can Disable Password IT policy rule.....	9
	BlackBerry App World policy group.....	10
	Enable Wireless Service Provider Billing IT policy rule.....	10
	Camera policy group.....	10
	Disable Photo Camera IT policy rule.....	10
	Disable Video Camera IT policy rule.....	10
	Password policy group.....	11
	Forbidden Passwords IT policy rule.....	11
	Maximum Password History IT policy rule.....	11
	Periodic Challenge Time IT policy rule.....	11
	Set Maximum Password Attempts IT policy rule.....	12
	Set Password Timeout IT policy rule.....	12
	Suppress Password Echo IT policy rule.....	13
	Personal Devices policy group.....	13
	Enable Separation of Work Content IT policy rule.....	13
	Work Domains IT policy rule.....	14
	Disable Forwarding of Work Content Using Personal Channels IT policy rule.....	14
	Require Work Resources for Conducting Work Activities IT policy rule.....	14
	PIM Synchronization policy group.....	15
	Disable All Wireless Synchronization IT policy rule.....	15
	Security policy group.....	15
	Content Protection Strength IT policy rule.....	15
	Disable External Memory IT policy rule.....	16
	External File System Encryption Level IT policy rule.....	16

Required Password Pattern IT policy rule.....	17
Wired Software Updates policy group.....	17
Allow Web-Based Software Loading IT policy rule.....	17
3 Configuration settings.....	19
Configuration settings for VPN profiles.....	19
Enable VPN configuration setting.....	19
Split-tunneling Mode configuration setting.....	19
Suppress VPN Banner configuration setting.....	19
Use VPN Xauth configuration setting.....	20
VPN Allow Handheld Changes configuration setting.....	20
VPN Allow Password Save configuration setting.....	20
VPN Disable Server Certificate Validation configuration setting.....	21
VPN DNS Configuration configuration setting.....	21
VPN Domain Name configuration setting.....	21
VPN Gateway Address configuration setting.....	22
VPN Group Name configuration setting.....	22
VPN Group Password configuration setting.....	22
VPN Hard Token Required configuration setting.....	22
VPN IKE Cipher configuration setting.....	23
VPN IKE DH Group configuration setting.....	23
VPN IKE Hash configuration setting.....	23
VPN IP Address configuration setting.....	24
VPN IPSec Cipher and Hash configuration setting.....	24
VPN Minimal Certificate Encryption Key Security Level configuration setting.....	25
VPN NAT Keep Alive configuration setting.....	25
VPN PFS configuration setting.....	25
VPN Primary DNS configuration setting.....	26
VPN Profile Editability configuration setting.....	26
VPN Profile Visibility configuration setting.....	26
VPN Secondary DNS configuration setting.....	27
VPN Subnet 1 IP Address configuration setting.....	27
VPN Subnet 1 Mask configuration setting.....	27
VPN Subnet 2 IP Address configuration setting.....	28
VPN Subnet 2 Mask configuration setting.....	28
VPN Subnet 3 IP Address configuration setting.....	28
VPN Subnet 3 Mask configuration setting.....	28
VPN Subnet Mask configuration setting.....	28
VPN Token Serial Number configuration setting.....	29

VPN User Name configuration setting.....	29
VPN User Password configuration setting.....	29
VPN Vendor Type configuration setting.....	30
VPN Xauth Type configuration setting.....	30
Configuration settings for Wi-Fi profiles.....	31
Associated Certificate Authority Configuration configuration setting.....	31
Wi-Fi Allow AP to AP Handover configuration setting.....	31
Wi-Fi Allow Handheld Changes configuration setting.....	31
Wi-Fi Allow Password Save configuration setting.....	32
Wi-Fi Band Type configuration setting.....	32
Wi-Fi BlackBerry Infrastructure Wi-Fi Access Mode configuration setting.....	32
Wi-Fi Default Gateway configuration setting.....	33
Wi-Fi Default Key ID configuration setting.....	33
Wi-Fi DHCP Configuration configuration setting.....	33
Wi-Fi Disable Server Certificate Validation configuration setting.....	34
Wi-Fi Domain Suffix configuration setting.....	34
Wi-Fi EAP-FAST Provisioning method configuration setting.....	34
Wi-Fi Enable Authentication Page configuration setting.....	35
Wi-Fi Hard Token Required configuration setting.....	35
Wi-Fi Inner Authentication Mode configuration setting.....	35
Wi-Fi Internet Access Path configuration setting.....	36
Wi-Fi IP Address configuration setting.....	36
Wi-Fi Link Security configuration setting.....	36
Wi-Fi Minimal EAP-TLS Certificate Encryption Key Security Level configuration setting.....	37
Wi-Fi Preshared Key configuration setting.....	38
Wi-Fi Primary DNS configuration setting.....	38
Wi-Fi Profile Editability configuration setting.....	38
Wi-Fi Profile Visibility configuration setting.....	39
Wi-Fi Roaming Threshold configuration setting.....	39
Wi-Fi Secondary DNS configuration setting.....	39
Wi-Fi Server SAN configuration setting.....	40
Wi-Fi Server Subject configuration setting.....	40
Wi-Fi SSID configuration setting.....	40
Wi-Fi Subnet Mask configuration setting.....	40
Wi-Fi Token Serial Number configuration setting.....	41
Wi-Fi User Name configuration setting.....	41
Wi-Fi User Password configuration setting.....	41
Wi-Fi WEP Key 1 configuration setting.....	41
Wi-Fi WEP Key 2 configuration setting.....	42

Wi-Fi WEP Key 3 configuration setting.....	42
Wi-Fi WEP Key 4 configuration setting.....	42
4 Examples of security goals.....	43
Requiring the use of a password on a device.....	43
Preventing the unauthorized use of a device.....	43
5 Glossary.....	44
6 Provide feedback.....	47
7 Legal notice.....	48

IT policy rules

1

You can assign IT policies to BlackBerry devices to meet your organization's security policy requirements and the needs of the BlackBerry device users in your organization's environment.

Preconfigured IT policies

The BlackBerry Business Cloud Services includes the following preconfigured IT policies that you can use to meet the requirements of your organization.

Preconfigured IT policy	Description
Default	This policy includes all the standard IT policy rules that are set in the BlackBerry Business Cloud Services.
Basic Password Security	This policy requires a basic password that users can use to unlock their BlackBerry devices. Users must change the passwords regularly. The IT policy includes a password timeout that locks devices.

Default values for preconfigured IT policies

You can configure additional IT policy rules in the preconfigured IT policies or change any of the following values:

IT policy rule	Default IT policy	Basic Password Security IT Policy
Device-Only Items		
Enable Long-Term Timeout	—	—
Maximum Security Timeout	—	30 minutes
Maximum Password Age	—	60 days
Minimum Password Length	—	—
Password Pattern Checks	No restriction	No restriction
Password Required	No	Yes
User Can Change Timeout	Yes	Yes
User Can Disable Password	Yes	No
Password policy group		
Forbidden Passwords	—	—
Maximum Password History	—	—
Periodic Challenge Time	—	—
Set Maximum Password Attempts	—	—
Set Password Timeout	—	—
Suppress Password Echo	—	—
Personal devices policy group		

IT policy rule	Default IT policy	Basic Password Security IT Policy
Enable Separation of Work Content	—	—
Disable Forwarding of Work Content Using Personal Channels	—	—
Require Work Resources for Conducting Work Activities	—	—
Work Domains	—	—
Security policy group		
Content Protection Strength	—	—
Disable External Memory	No	—
External File System Encryption level	Not required	—
Required Password Pattern	No	—
BlackBerry App World policy group		
Enable Wireless Service Provider Billing	—	—
Camera policy group		
Disable Photo Camera	—	—
Disable Video Camera	—	—
PIM Synchronization policy group		
Disable All Wireless Synchronization	—	—
Wired Software Updates policy group		
Allow Web-Based Software Loading	—	—

Descriptions of IT policy rules

Device Only policy group

Enable Long-Term Timeout IT policy rule

Description	This rule specifies whether a BlackBerry device locks after a predefined period of time, regardless of whether the BlackBerry device user is using the device.
Related rules	The Periodic Challenge Time IT policy rule affects this rule. Use the Periodic Challenge Time IT policy rule to shorten or extend the timeout interval.
Possible values	<ul style="list-style-type: none"> • Yes • No
Default values	<ul style="list-style-type: none"> • No
Minimum requirements	<ul style="list-style-type: none"> • BlackBerry Device Software 4.5

Maximum Password Age IT policy rule

Description	This rule specifies the number of days before a BlackBerry device password expires and a BlackBerry device user must set a new password. If you configure this rule to 0, the device password does not expire.
Related IT policy rules	The Password Required IT policy rule affects this rule. A device uses this rule only if the Password Required IT policy rule is configured to Yes.
Possible values	<ul style="list-style-type: none"> • 0 to 65,535 days
Default values	<ul style="list-style-type: none"> • 0 days in the Default IT policy • 60 days in the Basic Password Security IT policy
Minimum requirements	<ul style="list-style-type: none"> • BlackBerry Device Software 4.5

Maximum Security Timeout IT policy rule

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

	The User Can Change Timeout IT policy rule affects this rule. A user can specify any timeout value that is less than the maximum value, unless you configure the User Can Change Timeout IT policy rule to No.
Possible values	<ul style="list-style-type: none"> 10 to 480 minutes
Default values	<ul style="list-style-type: none"> Null value in the Default IT policy 30 minutes in the Basic Password Security IT policy
Minimum requirements	<ul style="list-style-type: none"> BlackBerry Device Software 4.5

Minimum Password Length IT policy rule

Description	<p>This rule specifies the minimum number of characters that are required for a BlackBerry device password.</p> <p>This rule does not control the maximum number of characters for the password. The maximum number is 32 characters.</p>
Related rules	The Password Required IT policy rule affects this rule. A device uses this rule only if the Password Required IT policy rule is configured to Yes.
Possible values	<ul style="list-style-type: none"> 4 to 14 characters
Default value	<ul style="list-style-type: none"> Null value
Minimum requirements	<ul style="list-style-type: none"> BlackBerry Device Software 4.5

Password Pattern Checks IT policy rule

Description	This rule specifies whether to verify that a BlackBerry device password matches specific character-pattern requirements. By default, a device prevents a BlackBerry device user from setting a password that uses a natural sequence of characters or numbers. If a symbol is inserted into a natural sequence, a device can use the password.
Related rules	The Password Required IT policy rule affects this rule. A device uses this rule only if the Password Required IT policy rule is configured to Yes.
Possible values	<ul style="list-style-type: none"> At least 1 alpha and 1 numeric character At least 1 alpha, 1 numeric, and 1 special character At least 1 upper-case alpha, 1 lower-case alpha, 1 numeric, and 1 special character No restriction
Default values	<ul style="list-style-type: none"> No restriction

Minimum requirements	<ul style="list-style-type: none"> BlackBerry Device Software 4.5
-----------------------------	--

Password Required IT policy rule

Description	This rule specifies whether a BlackBerry device user must configure a password on a BlackBerry device.
Possible values	<ul style="list-style-type: none"> Yes No
Default values	<ul style="list-style-type: none"> No in the Default IT policy Yes in the Basic Password Security IT policy
Minimum requirements	<ul style="list-style-type: none"> BlackBerry Device Software 4.5

User Can Change Timeout IT policy rule

Description	This rule specifies whether a BlackBerry device user can override the security timeout value.
Possible values	<ul style="list-style-type: none"> Yes No
Default value	<ul style="list-style-type: none"> Yes
Minimum requirements	<ul style="list-style-type: none"> BlackBerry Device Software 4.5

User Can Disable Password IT policy rule

Description	This rule specifies whether a BlackBerry device user can turn off the requirement for a password on a BlackBerry device.
Related rules	The Password Required IT policy rule affects this rule. A device uses this rule only if the Password Required IT policy rule is configured to Yes.
Possible values	<ul style="list-style-type: none"> Yes No
Default values	<ul style="list-style-type: none"> Yes in the Default IT policy No in the Basic Password Security IT policy rule
Minimum requirements	<ul style="list-style-type: none"> BlackBerry Device Software 4.5

BlackBerry App World policy group

Enable Wireless Service Provider Billing IT policy rule

Description	This rule specifies whether a BlackBerry device user can purchase applications from the BlackBerry App World storefront using the purchasing plan for your organization's wireless service provider.
Possible values	<ul style="list-style-type: none"> • Yes • No
Default values	<ul style="list-style-type: none"> • No
Minimum requirements	<ul style="list-style-type: none"> • BlackBerry Device Software 4.5

Camera policy group

Disable Photo Camera IT policy rule

Description	This rule specifies whether the camera on a BlackBerry device is turned on.
Possible values	<ul style="list-style-type: none"> • Yes • No
Default value	<ul style="list-style-type: none"> • No
Minimum requirements	<ul style="list-style-type: none"> • BlackBerry Device Software 4.5

Disable Video Camera IT policy rule

Description	This rule specifies whether the video camera on a BlackBerry device is turned on.
Possible values	<ul style="list-style-type: none"> • Yes • No
Default value	<ul style="list-style-type: none"> • No
Minimum requirements	<ul style="list-style-type: none"> • BlackBerry Device Software 4.5

Password policy group

A BlackBerry device uses the IT policy rules in the Password policy group only if you configure the Password Required IT policy rule to Yes in the Device Only policy group.

Forbidden Passwords IT policy rule

Description	This rule specifies the passwords that a BlackBerry device user cannot use. Separate multiple passwords with a comma (.). By default, a BlackBerry device prevents a user from configuring passwords that use a natural sequence of characters or numbers. The device also automatically prevents common letter substitutions. For example, if you include "password" in the forbidden passwords list, users cannot use "p@ssw0rd", "pa\$zword", or "password123" on the device.
Related rules	The Password Required IT policy rule affects this rule. The device uses this rule only if you set the Password Required IT policy rule to Yes.
Default value	<ul style="list-style-type: none"> Null value
Minimum requirements	<ul style="list-style-type: none"> BlackBerry Device Software 4.5

Maximum Password History IT policy rule

Description	This rule specifies the maximum number of previous passwords that a BlackBerry device checks new passwords against to prevent a BlackBerry device user from reusing previous passwords.
Related rules	The Password Required IT policy rule affects this rule. The device uses this rule only if you set the Password Required IT policy rule to Yes.
Possible values	<ul style="list-style-type: none"> 0 to 15 passwords
Default values	<ul style="list-style-type: none"> 0
Minimum requirements	<ul style="list-style-type: none"> BlackBerry Device Software 4.5

Periodic Challenge Time IT policy rule

Description	This rule specifies the security timeout interval that must elapse before a BlackBerry device locks and prompts a BlackBerry device user to type a password, regardless of whether the device was active during that interval.
Related rules	The Password Required IT policy rule affects this rule. The device uses this rule only if you set the Password Required IT policy rule to Yes.

	<p>The User Can Change Timeout IT policy rule affects this rule. Change the User Can Change Timeout IT policy rule to No so that a user cannot change the timeout settings on a device.</p> <p>The Enable Long-Term Timeout IT policy rule affects this rule. By default, if you change the Enable Long-Term Timeout IT policy rule to Yes, the security timeout interval is turned on and set to 60 minutes.</p>
Possible values	<ul style="list-style-type: none"> 1 to 1440 minutes
Default value	<ul style="list-style-type: none"> 60 minutes
Minimum requirements	<ul style="list-style-type: none"> BlackBerry Device Software 4.5

Set Maximum Password Attempts IT policy rule

Description	This rule specifies the number of times that a BlackBerry device user can try a password before a BlackBerry device permanently deletes all of the application data.
Related rules	The Password Required IT policy rule affects this rule. The device uses this rule only if you set the Password Required IT policy rule to Yes.
Possible values	<ul style="list-style-type: none"> 3 to 10
Default value	<ul style="list-style-type: none"> 10
Minimum requirements	<ul style="list-style-type: none"> BlackBerry Device Software 4.5

Set Password Timeout IT policy rule

Description	This rule specifies the amount of time of inactivity that can occur before a BlackBerry device user must type the password to unlock a BlackBerry device. This rule defines the default value for the security timeout.
Related rules	The User Can Change Timeout IT policy rule affects this rule. If you set the User Can Change Timeout IT policy rule to No, the device uses the security timeout that you set in this rule.
Possible values	<ul style="list-style-type: none"> 0 to 60 minutes
Default value	<ul style="list-style-type: none"> 2 minutes for BlackBerry Device Software 4.6 and earlier 30 minutes for BlackBerry Device Software 4.7 and later
Minimum requirements	<ul style="list-style-type: none"> BlackBerry Device Software 4.5

Suppress Password Echo IT policy rule

Description	This rule specifies whether the characters that a BlackBerry device user types in the Password dialog box appear on the BlackBerry device screen after the user types the password incorrectly a specific number of times.
Related rules	<p>The Password Required IT policy rule affects this rule. The device uses this rule only if a password is configured on the device. To require a password, configure the Password Required IT policy rule to Yes.</p> <p>The Set Maximum Password Attempts IT policy rule affects this rule. To specify the number of times that the user can type the password incorrectly before the characters appear on the screen, configure the Set Maximum Password Attempts IT policy rule.</p>
Possible values	<ul style="list-style-type: none"> • Yes • No
Default value	<ul style="list-style-type: none"> • No
Minimum requirements	<ul style="list-style-type: none"> • BlackBerry Device Software 4.5

Personal Devices policy group

Enable Separation of Work Content IT policy rule

Description	This rule specifies whether a BlackBerry device distinguishes between work data and personal data, and whether only authorized applications on the device can access work data. If you set this rule to Yes and a BlackBerry device user tries to delete a desktop service book, the device prompts the user to delete the work data on the device.
Possible values	<ul style="list-style-type: none"> • Yes • No
Default value	<ul style="list-style-type: none"> • No
Minimum requirements	<ul style="list-style-type: none"> • BlackBerry 6

Work Domains IT policy rule

Description	<p>This rule specifies a list of resources (for example, domain names, server names, and email-address domains) that a BlackBerry device identifies as work resources. If you list a domain, all of the subdomains of the domain are included automatically. If you list multiple resources, separate the resources with a comma (,), semicolon (;), or space. For example, if your organization has multiple domains, type example.com, example.net, example.org.</p> <p>If you set this rule, the device warns a BlackBerry device user when an email message includes an email address that does not belong to a work domain. The device highlights email addresses that do not belong to the work domain in yellow. If the user tries to forward a work email to an email address that does not belong to the work domain or includes an email address that does not belong to the work domain to a reply, the device also displays a warning message.</p>
Default value	<ul style="list-style-type: none"> Null value
Minimum requirements	<ul style="list-style-type: none"> BlackBerry 6

Disable Forwarding of Work Content Using Personal Channels IT policy rule

Description	<p>This rule specifies whether a BlackBerry device user can send work data to contacts using personal resources (for example, SMS text messages, MMS messages, or email messages from personal email accounts).</p>
Related rules	<p>The Enable Separation of Work Content IT policy rule affects this rule. A BlackBerry device only uses this rule if you set the Enable Separation of Work Content IT policy rule to Yes.</p>
Possible values	<ul style="list-style-type: none"> Yes No
Default value	<ul style="list-style-type: none"> No
Minimum requirements	<ul style="list-style-type: none"> BlackBerry 6

Require Work Resources for Conducting Work Activities IT policy rule

Description	<p>This rule specifies whether a BlackBerry device must use work resources (for example, work email accounts or work calendars) when a BlackBerry device user conducts work activity (for example, sending an email message to a work contact or scheduling a work appointment).</p>
Related rules	<p>The Enable Separation of Work Content IT policy rule affects this rule. The device only uses this rule if you set the Enable Separation of Work Content IT policy rule to Yes.</p>
Possible values	<ul style="list-style-type: none"> Yes

	<ul style="list-style-type: none"> No
Default value	<ul style="list-style-type: none"> No
Minimum requirements	<ul style="list-style-type: none"> BlackBerry 6

PIM Synchronization policy group

Disable All Wireless Synchronization IT policy rule

Description	<p>This rule specifies whether wireless data synchronization is turned off. Set this rule to Yes to turn off all wireless data synchronization, except wireless email reconciliation. This rule prevents the following actions:</p> <ul style="list-style-type: none"> Wireless synchronization of contact entries, calendar entries, email filters, tasks, and memos Wireless synchronization of all logging information Wireless backup of data, including configuration data for BlackBerry devices Wireless bulk loads Activation of devices over the wireless network
Possible values	<ul style="list-style-type: none"> Yes No
Default value	<ul style="list-style-type: none"> No
Minimum requirements	<ul style="list-style-type: none"> BlackBerry Device Software 4.5

Security policy group

Content Protection Strength IT policy rule

Description	<p>This rule specifies the cryptographic strength that a BlackBerry device uses for content protection of data that it receives when it is locked. When you specify a value for this rule, content protection is turned on. If you set this rule to Strong, the device uses a 160-bit ECC public key. If you set this rule to Stronger, the device uses a 283-bit ECC public key. If you set this rule to Strongest, the device uses a 571-bit ECC public key.</p> <p>For devices that are running BlackBerry Device Software 5.0 and later with onboard device memory, this rule also encrypts the onboard device memory using the BlackBerry device user password and a device-generated key. Media files in the onboard device memory are not encrypted.</p>
--------------------	---

	For devices that are running BlackBerry Device Software 4.7 and earlier, you can configure the External File System Encryption Level IT policy rule to encrypt media files on the media card.
Related rules	<p>The Password Required IT policy rule affects this rule. A device uses this rule only if you set the Password Required IT policy rule to Yes.</p> <p>This rule affects the Minimum Password Length IT policy rule. If you set this rule to Stronger, you should set the Minimum Password Length IT policy rule to 12 characters. If you set this rule to Strongest, you should set the Minimum Password Length IT policy rule to 21 characters.</p>
Possible values	<ul style="list-style-type: none"> • Strong • Stronger • Strongest
Default values	<ul style="list-style-type: none"> • Null value
Minimum requirements	<ul style="list-style-type: none"> • BlackBerry Device Software 4.5

Disable External Memory IT policy rule

Description	This rule specifies whether to prevent a BlackBerry device user from accessing the media card on a BlackBerry device.
Possible values	<ul style="list-style-type: none"> • Yes • No
Default value	<ul style="list-style-type: none"> • No
Minimum requirements	<ul style="list-style-type: none"> • BlackBerry Device Software 4.5

External File System Encryption Level IT policy rule

Description	<p>This rule specifies the level of encryption that a BlackBerry device uses to encrypt files that it stores on a media card. You can use this rule to require that the device encrypts a media card, either including or excluding media-card files. You cannot use this rule to encrypt files that a BlackBerry device user transfers to the media card manually (for example, from a USB mass storage device).</p> <p>The master keys for the media card are stored on the media card. A device is designed to use the master keys to decrypt and encrypt files on the media card. A device is designed to use the device key, a user-provided password, or both to encrypt the master keys.</p>
Possible values	<ul style="list-style-type: none"> • Encrypt to User Password (excluding multimedia directories) • Encrypt to User Password (including multimedia directories) • Encrypt to Device Key (excluding multimedia directories) • Encrypt to Device Key (including multimedia directories)

	<ul style="list-style-type: none"> • Encrypt to User Password and Device Key (excluding multimedia directories) • Encrypt to User Password and Device Key (including multimedia directories) • Not required
Default values	<ul style="list-style-type: none"> • Not required
Minimum requirements	<ul style="list-style-type: none"> • BlackBerry Device Software 4.5

Required Password Pattern IT policy rule

Description	<p>This rule specifies the required pattern for a BlackBerry device password. A character in the password pattern specifies the character type permitted in its position in the password. Passwords can contain Latin-1 characters only. If you configure this rule, a BlackBerry device user can only create a password that is greater than or equal to the length of the pattern on the device. Password characters that exceed the pattern length can be letters, numbers, or symbols.</p> <p>You can use the following characters to specify the password pattern:</p> <ul style="list-style-type: none"> • a: Permits any letter • A: Permits an uppercase letter only • c: Permits any consonant letter • C: Permits an uppercase consonant letter only • v: Permits any vowel • V: Permits an uppercase vowel only • N, n, or #: Permits a number only • S, s, or @: Permits a symbol only • ?: Permits any letter, number, or symbol
Default value	<ul style="list-style-type: none"> • Null value
Minimum requirements	<ul style="list-style-type: none"> • BlackBerry Device Software 4.5

Wired Software Updates policy group

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

Allow Web-Based Software Loading IT policy rule

Description	<p>This rule specifies whether a BlackBerry device user can update the BlackBerry Device Software using software loading feature over the Internet.</p>
--------------------	---

Possible values	<ul style="list-style-type: none">• Yes• No
Default value	<ul style="list-style-type: none">• No
Minimum requirements	<ul style="list-style-type: none">• BlackBerry Device Software 5.0

Configuration settings

Configuration settings for VPN profiles

Enable VPN configuration setting

Description	This setting specifies whether the VPN client on a BlackBerry device is turned on. If you change this setting to Yes, the device must use a VPN server to access a Wi-Fi network. If you change this setting to No, the device might not be able to use a Wi-Fi network that requires VPN access, or it might require the use of an alternative form of access control.
Possible values	<ul style="list-style-type: none"> • Yes • No
Default value	<ul style="list-style-type: none"> • No
Minimum requirements	<ul style="list-style-type: none"> • BlackBerry Device Software 4.5

Split-tunneling Mode configuration setting

Description	This setting specifies whether a BlackBerry device can use split-tunneling to bypass an active VPN connection.
Possible values	<ul style="list-style-type: none"> • Enable on all networks • Disable on corporate networks • Disable on all networks
Default value	<ul style="list-style-type: none"> • Disable on all networks
Minimum requirements	<ul style="list-style-type: none"> • BlackBerry Device Software 5.0

Suppress VPN Banner configuration setting

Description	This setting specifies whether the VPN dialog box displays on a BlackBerry device after the device connects to a VPN server.
Possible values	<ul style="list-style-type: none"> • Yes • No
Default value	<ul style="list-style-type: none"> • Yes
Minimum requirements	<ul style="list-style-type: none"> • BlackBerry Device Software 4.5

Use VPN Xauth configuration setting

Description	This setting specifies whether the VPN client on a BlackBerry device should use Xauth certificates to authenticate with your organization's VPN gateway.
Related settings	The Enable VPN configuration setting affects this configuration setting. You must change the Enable VPN configuration setting to Yes so that the device can use this configuration setting.
Possible values	<ul style="list-style-type: none"> • Yes • No
Default value	<ul style="list-style-type: none"> • No
Minimum requirements	<ul style="list-style-type: none"> • BlackBerry Device Software 4.5

VPN Allow Handheld Changes configuration setting

Description	<p>This setting specifies whether a BlackBerry device user can change all of the VPN policy rules on a BlackBerry device.</p> <p>If you change this setting to No, a user can continue to change the VPN user name and VPN password on the device.</p>
Possible values	<ul style="list-style-type: none"> • Yes • No
Default value	<ul style="list-style-type: none"> • Yes
Minimum requirements	<ul style="list-style-type: none"> • BlackBerry Device Software 4.5

VPN Allow Password Save configuration setting

Description	This setting specifies whether a BlackBerry device user can save the VPN password on a BlackBerry device.
Possible values	<ul style="list-style-type: none"> • Yes • No
Default value	<ul style="list-style-type: none"> • Yes
Minimum requirements	<ul style="list-style-type: none"> • BlackBerry Device Software 4.5

VPN Disable Server Certificate Validation configuration setting

Description	This setting specifies whether a BlackBerry device requires a certificate to authenticate with VPN gateways that support PKI-based authentication using certificates. This setting applies to the following VPN gateways that support PKI-based authentication using certificates: the Cisco Secure PIX Firewall, Cisco IOS with Easy VPN Server, NetScreen Series Security Systems, and Nortel Networks Contivity VPN switch.
Possible values	<ul style="list-style-type: none"> • Yes • No
Default value	<ul style="list-style-type: none"> • No
Minimum requirements	<ul style="list-style-type: none"> • BlackBerry Device Software 5.0

VPN DNS Configuration configuration setting

Description	This setting specifies your organization's VPN DNS configuration. To require that a BlackBerry device retrieves DNS settings from the VPN gateway, change this setting to Yes. To require that the device uses the static settings that are specified in the VPN Primary DNS configuration setting, VPN Secondary DNS configuration setting, and VPN Domain Name configuration setting, change this setting to No.
Related settings	The Enable VPN configuration setting affects this configuration setting. You must set the Enable VPN configuration setting to Yes so that the device uses this configuration setting.
Possible values	<ul style="list-style-type: none"> • Yes • No
Default setting	<ul style="list-style-type: none"> • Yes
Minimum requirements	<ul style="list-style-type: none"> • BlackBerry Device Software 4.5

VPN Domain Name configuration setting

Description	This setting specifies the suffix for your organization's domain name using the FQDN format.
Related settings	<p>The Enable VPN configuration setting affects this configuration setting. You must set the Enable VPN configuration setting to Yes so that a BlackBerry device uses this configuration setting.</p> <p>The VPN DNS Configuration configuration setting affects this configuration setting. You must set the VPN DNS Configuration configuration setting to No so that the device uses this configuration setting.</p>
Default value	<ul style="list-style-type: none"> • Null value

Minimum requirements	<ul style="list-style-type: none"> BlackBerry Device Software 4.5
-----------------------------	--

VPN Gateway Address configuration setting

Description	This setting specifies the IP address or FQDN of your organization's VPN server.
Default value	<ul style="list-style-type: none"> Null value
Minimum requirements	<ul style="list-style-type: none"> BlackBerry Device Software 4.5

VPN Group Name configuration setting

Description	This setting specifies the group name of your organization's VPN server. Specify the group name for your organization's VPN server only if the VPN client requires it.
Default value	<ul style="list-style-type: none"> Null value
Minimum requirements	<ul style="list-style-type: none"> BlackBerry Device Software 4.5

VPN Group Password configuration setting

Description	This setting specifies the group password for your organization's VPN server. Specify the group password for your organization's VPN server only if the VPN client requires it.
Default value	<ul style="list-style-type: none"> Null value
Minimum requirements	<ul style="list-style-type: none"> BlackBerry Device Software 4.5

VPN Hard Token Required configuration setting

Description	This setting specifies whether the VPN server requires that a BlackBerry device uses a hard token as part of the password for authentication.
Possible values	<ul style="list-style-type: none"> Yes No
Default value	<ul style="list-style-type: none"> No
Minimum requirements	<ul style="list-style-type: none"> BlackBerry Device Software 4.5

VPN IKE Cipher configuration setting

Description	This setting specifies the encryption algorithm that a BlackBerry device uses to authenticate IKE exchanges. Change this setting only if the encryption algorithm does not support AES128.
Possible values	<ul style="list-style-type: none"> • DES • 3DES • AES128 • AES192 • AES256
Default value	<ul style="list-style-type: none"> • AES128
Minimum requirements	<ul style="list-style-type: none"> • BlackBerry Device Software 4.5

VPN IKE DH Group configuration setting

Description	This setting specifies the DH group that a BlackBerry device uses to generate key material. Change this setting only if the the DH group does not use ECC.
Related settings	The Enable VPN configuration setting affects this rule. You must change the Enable VPN configuration setting to Yes so that the device can use this setting.
Possible values	<ul style="list-style-type: none"> • Group 1 • Group 2 • Group 5 • Group 7 • Group 9
Default value	<ul style="list-style-type: none"> • Group 7
Minimum requirements	<ul style="list-style-type: none"> • BlackBerry Device Software 4.5

VPN IKE Hash configuration setting

Description	This setting specifies the hash method authentication code that a BlackBerry device can use. Change this setting only if the hash method authentication code does not support SHA1 160 bits.
Possible values	<ul style="list-style-type: none"> • MD5 128 bits • SHA1 160 bits
Default value	<ul style="list-style-type: none"> • SHA1 160 bits
Minimum requirements	<ul style="list-style-type: none"> • BlackBerry Device Software 4.5

VPN IP Address configuration setting

Description	This setting specifies the IP address of the VPN.
Default value	<ul style="list-style-type: none"> Null value
Minimum requirements	<ul style="list-style-type: none"> BlackBerry Device Software 4.5

VPN IPSec Cipher and Hash configuration setting

Description	This setting specifies the encryption algorithm and hash that a BlackBerry device uses for IPSec Security Associations. Change this setting only if the IPSec Hash and Cipher are not SHA1 Hash and AES128 Cipher.
Possible values	<ul style="list-style-type: none"> MD5 Hash with No Cipher SHA1 Hash with No Cipher No Hash with DES Cipher MD5 Hash and DES Cipher SHA1 Hash and DES Cipher No Hash and 3DES Cipher MD5 Hash and 3DES Cipher SHA1 Hash and 3DES Cipher No Hash and AES128 Cipher MD5 Hash and AES128 Cipher SHA1 Hash and AES128 Cipher No Hash and AES192 Cipher MD5 Hash and AES192 Cipher SHA1 Hash and AES192 Cipher No Hash and AES256 Cipher MD5 Hash and AES256 Cipher SHA1 Hash and AES256 Cipher
Default value	<ul style="list-style-type: none"> SHA1 Hash and AES128 Cipher
Minimum requirements	<ul style="list-style-type: none"> BlackBerry Device Software 4.5

VPN Minimal Certificate Encryption Key Security Level configuration setting

Description	<p>This setting specifies the minimum security level for private keys that a BlackBerry device uses for authentication methods that require client certificates.</p> <p>If you change this setting to High security, the device always prompts a BlackBerry device user for the key store password when the device requires access to the private key. This might happen frequently, even if the user types the password recently. Private keys are not stored with the VPN profile.</p> <p>If you change this setting to Medium security, the device prompts the user for the key store password the first time and then prompts the user only after the user resets the device. Private keys are cached in memory but are not stored with the VPN profile.</p> <p>If you change this setting to Low security, A device prompts the user for the key store password only once. The device retrieves and stores the private key in unencrypted format with the VPN profile.</p>
Possible values	<ul style="list-style-type: none"> • Low security • High security • Medium security
Default value	<ul style="list-style-type: none"> • Low security
Minimum requirements	<ul style="list-style-type: none"> • BlackBerry Device Software 4.5

VPN NAT Keep Alive configuration setting

Description	<p>This setting specifies the NAT keep-alive frequency. Specify the interval that a BlackBerry device sends a keep-alive packet to the VPN concentrator to maintain the connection to the VPN concentrator.</p>
Possible values	<ul style="list-style-type: none"> • 1 to 1439 minutes
Default value	<ul style="list-style-type: none"> • 1 minute
Minimum requirements	<ul style="list-style-type: none"> • BlackBerry Device Software 4.5

VPN PFS configuration setting

Description	<p>This setting specifies whether PFS is turned on for a BlackBerry device. Change this setting only if your organization does not support PFS.</p>
--------------------	---

Possible values	<ul style="list-style-type: none"> • Yes • No
Default value	<ul style="list-style-type: none"> • Yes
Minimum requirements	<ul style="list-style-type: none"> • BlackBerry Device Software 4.5

VPN Primary DNS configuration setting

Description	This setting specifies the static setting for the IP address of your organization's primary DNS server.
Related settings	<p>The Enable VPN configuration setting affects this configuration setting. You must change the Enable VPN configuration setting to Yes so that a BlackBerry device can use this configuration setting.</p> <p>The VPN DNS Configuration configuration setting affects this configuration setting. You must change the VPN DNS Configuration configuration setting to No so that the device can use this configuration setting.</p>
Default value	<ul style="list-style-type: none"> • Null value
Minimum requirements	<ul style="list-style-type: none"> • BlackBerry Device Software 4.5

VPN Profile Editability configuration setting

Description	This setting specifies whether a BlackBerry device user can change the configuration settings of the VPN profile on a BlackBerry device.
Possible values	<ul style="list-style-type: none"> • Full editability • No editability • Credentials editability
Default value	<ul style="list-style-type: none"> • Full editability
Minimum requirements	<ul style="list-style-type: none"> • BlackBerry Device Software 4.5

VPN Profile Visibility configuration setting

Description	This setting specifies whether a BlackBerry device user can view the configuration settings of the VPN profile on a BlackBerry device.
Possible values	<ul style="list-style-type: none"> • Full visibility • Restricted visibility

	<ul style="list-style-type: none"> • Credentials visibility
Default value	<ul style="list-style-type: none"> • Full visibility
Minimum requirements	<ul style="list-style-type: none"> • BlackBerry Device Software 4.5

VPN Secondary DNS configuration setting

Description	This setting specifies the static setting for the IP address of your organization's secondary DNS server.
Related settings	<p>The Enable VPN configuration setting affects this configuration setting. You must change the Enable VPN configuration setting to Yes so that a BlackBerry device can use this setting.</p> <p>The VPN DNS Configuration configuration setting affects this configuration setting. You must change the VPN DNS Configuration configuration setting to No so that the device can use this setting.</p>
Default value	<ul style="list-style-type: none"> • Null value
Minimum requirements	<ul style="list-style-type: none"> • BlackBerry Device Software 4.5

VPN Subnet 1 IP Address configuration setting

Description	This setting specifies the IP address of subnet 1 for VPN gateways that require a BlackBerry device to specify a subnet. Type the IP address in dot-decimal notation (for example, 192.0.2.1).
Default value	<ul style="list-style-type: none"> • Null value
Minimum requirements	<ul style="list-style-type: none"> • BlackBerry Device Software 4.6

VPN Subnet 1 Mask configuration setting

Description	This setting specifies the subnet mask of subnet 1 for VPN gateways that require a BlackBerry device to specify a subnet.
Default value	<ul style="list-style-type: none"> • Null value
Minimum requirements	<ul style="list-style-type: none"> • BlackBerry Device Software 4.6

VPN Subnet 2 IP Address configuration setting

Description	This setting specifies the IP address of subnet 2 for VPN gateways that require a BlackBerry device to specify a subnet. Type the IP address in dot-decimal notation (for example, 192.0.2.1).
Default value	<ul style="list-style-type: none"> Null value
Minimum requirements	<ul style="list-style-type: none"> BlackBerry Device Software 4.6

VPN Subnet 2 Mask configuration setting

Description	This setting specifies the subnet mask of subnet 2 for VPN gateways that require a BlackBerry device to specify a subnet.
Default value	<ul style="list-style-type: none"> Null value
Minimum requirements	<ul style="list-style-type: none"> BlackBerry Device Software 4.6

VPN Subnet 3 IP Address configuration setting

Description	This setting specifies the IP address of subnet 3 for VPN gateways that require a BlackBerry device to specify a subnet. Type the IP address in dot-decimal notation (for example, 192.0.2.1).
Default value	<ul style="list-style-type: none"> Null value
Minimum requirements	<ul style="list-style-type: none"> BlackBerry Device Software 4.6

VPN Subnet 3 Mask configuration setting

Description	This setting specifies the subnet mask of subnet 3 for VPN gateways that require a BlackBerry device to specify a subnet.
Default value	<ul style="list-style-type: none"> Null value
Minimum requirements	<ul style="list-style-type: none"> BlackBerry Device Software 4.6

VPN Subnet Mask configuration setting

Description	This setting specifies the IP address of the subnet mask of the VPN.
--------------------	--

Related settings	<p>This configuration setting affects the Enable VPN configuration setting. If you change this configuration setting, you must set the Enable VPN configuration setting to Yes.</p> <p>This configuration setting affects the VPN DNS Configuration configuration setting. If you change this configuration setting, you must set the VPN DNS Configuration configuration setting to No.</p>
Default setting	<ul style="list-style-type: none"> Null value
Minimum requirements	<ul style="list-style-type: none"> BlackBerry Device Software 4.5

VPN Token Serial Number configuration setting

Description	<p>If the VPN server requires that a BlackBerry device uses a software token as part of the password for authentication, this setting specifies the serial number of the software token that is provisioned for the device.</p>
Default value	<ul style="list-style-type: none"> Null value
Minimum requirements	<ul style="list-style-type: none"> BlackBerry Device Software 4.5

VPN User Name configuration setting

Description	<p>This setting specifies the default user name that a BlackBerry device uses to log in to your organization's VPN server. Configure this setting if you want to create a default user name for all user accounts.</p> <p>If a BlackBerry device user types a user name on the device manually, IT policy updates overwrite or delete the value that the user typed. To retain the value that the user types on the device, verify that the updated configuration setting uses the same value as this setting.</p>
Related settings	<p>The Enable VPN configuration setting affects this configuration setting. You must change the Enable VPN configuration setting to Yes so that the device can use this setting.</p>
Default value	<ul style="list-style-type: none"> Null value
Minimum requirements	<ul style="list-style-type: none"> BlackBerry Device Software 4.5

VPN User Password configuration setting

Description	<p>This setting specifies the default password that a BlackBerry device uses to log in to your organization's VPN server. Configure this setting if you want to create a default password for all user accounts.</p>
--------------------	--

	If a BlackBerry device user types a password on the device manually, IT policy updates overwrite or delete the value that the user typed. To retain the value that the user types on the device, verify that the updated configuration setting uses the same value as this configuration setting.
Related settings	The Enable VPN configuration setting affects this configuration setting. You must change the Enable VPN configuration setting to Yes so that the device can use this configuration setting.
Default value	<ul style="list-style-type: none"> Null value
Minimum requirements	<ul style="list-style-type: none"> BlackBerry Device Software 4.5

VPN Vendor Type configuration setting

Description	This setting specifies the type of VPN client that the VPN client on a BlackBerry device emulates.
Related settings	The Enable VPN configuration setting affects this configuration setting. You must set the Enable VPN configuration setting to Yes so that the device can use this configuration setting.
Possible values	<ul style="list-style-type: none"> Alcatel 7130 Secure VPN Gateway Family Avaya VSU(TM) Series Check Point(TM) Software Technologies VPN-1 Cisco VPN Concentrator 3000 Series Cisco Secure PIX Firewall VPN Cisco IOS with Easy VPN Server Cosine IPX VPN Gateway Cylink Nethawk Intel®) Netstructure(TM) 3100 Series Lucent Firewall Brick Family Netscreen Systems Nortel Networks Contivity VPN Switch Series ReefEdge Connect Server Secure Computing Sidewinder(TM) Firewall Symantec Raptor Firewall and PowerVPN
Default value	<ul style="list-style-type: none"> Null value
Minimum requirements	<ul style="list-style-type: none"> BlackBerry Device Software 4.5

VPN Xauth Type configuration setting

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

Related settings	The Enable VPN configuration setting affects this configuration setting. You must change the Enable VPN configuration setting to Yes so that a BlackBerry device can use this configuration setting.
Possible values	<ul style="list-style-type: none"> User name and password required SecurID required
Default value	<ul style="list-style-type: none"> User name and password required
Minimum requirements	<ul style="list-style-type: none"> BlackBerry Device Software 4.5

Configuration settings for Wi-Fi profiles

Associated Certificate Authority Configuration configuration setting

Description	This setting specifies the name of the certificate authority profile in the Certificate Authority Profile Name IT policy rule. The certificate authority profile consists of credentials that a BlackBerry device can use to initiate a certificate-enrollment process. After you associate a certificate authority profile with a Wi-Fi profile, you can assign the Wi-Fi profile to a user account and send the profile to the device.
Default value	<ul style="list-style-type: none"> Null value
Minimum requirements	<ul style="list-style-type: none"> BlackBerry Device Software 5.0

Wi-Fi Allow AP to AP Handover configuration setting

Description	This setting specifies whether a BlackBerry device can perform Wi-Fi handovers between wireless access points.
Possible values	<ul style="list-style-type: none"> Yes No
Default value	<ul style="list-style-type: none"> Yes
Minimum requirements	<ul style="list-style-type: none"> BlackBerry Device Software 4.5

Wi-Fi Allow Handheld Changes configuration setting

Description	This setting specifies whether a BlackBerry device user can change the Wi-Fi policy settings on a BlackBerry device.
--------------------	--

Possible values	<ul style="list-style-type: none"> • Yes • No
Default value	<ul style="list-style-type: none"> • Yes
Minimum requirements	<ul style="list-style-type: none"> • BlackBerry Device Software 4.5

Wi-Fi Allow Password Save configuration setting

Description	This setting specifies whether a BlackBerry device user can save passwords for authentication to a Wi-Fi network on a BlackBerry device.
Possible values	<ul style="list-style-type: none"> • Yes • No
Default value	<ul style="list-style-type: none"> • Yes
Minimum requirements	<ul style="list-style-type: none"> • BlackBerry Device Software 4.5

Wi-Fi Band Type configuration setting

Description	This setting specifies the band types that you configure the wireless access points of a specific SSID to operate on.
Possible values	<ul style="list-style-type: none"> • 802.11 a/b/g • 802.11 b/g • 802.11 a • 802.11 b
Default value	<ul style="list-style-type: none"> • 802.11 a/b/g
Minimum requirements	<ul style="list-style-type: none"> • BlackBerry Device Software 4.5

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

Description	This setting specifies whether a BlackBerry device can connect to the BlackBerry Infrastructure over a Wi-Fi network.
Possible values	<ul style="list-style-type: none"> • Access does not require VPN • Access requires VPN • Access disabled
Default value	<ul style="list-style-type: none"> • Access does not require VPN

Minimum requirements	<ul style="list-style-type: none"> BlackBerry Device Software 5.0
-----------------------------	--

Wi-Fi Default Gateway configuration setting

Description	This setting specifies the default gateway in IP address format (for example, 10.0.0.1) that a BlackBerry device can use if DHCP on the device is turned off.
Related settings	The Wi-Fi DHCP Configuration configuration setting affects this configuration setting. The device uses this configuration setting only if you change the Wi-Fi DHCP Configuration configuration setting to No.
Default value	<ul style="list-style-type: none"> Null value
Minimum requirements	<ul style="list-style-type: none"> BlackBerry Device Software 4.5

Wi-Fi Default Key ID configuration setting

Description	This setting specifies the default WEP key ID. Verify that the WEP key ID matches the WEP access point ID and the corresponding WEP key.
Possible values	<ul style="list-style-type: none"> 1 to 4
Default value	<ul style="list-style-type: none"> 1
Minimum requirements	<ul style="list-style-type: none"> BlackBerry Device Software 4.5

Wi-Fi DHCP Configuration configuration setting

Description	This setting specifies whether your organization uses DHCP for dynamic network configuration. If your organization uses a Wi-Fi network that includes subnets, turn on DHCP to permit roaming between subnets.
Possible values	<ul style="list-style-type: none"> Yes No
Default value	<ul style="list-style-type: none"> Yes
Minimum requirements	<ul style="list-style-type: none"> BlackBerry Device Software 4.5

Wi-Fi Disable Server Certificate Validation configuration setting

Description	<p>This setting specifies whether a BlackBerry device requires a certificate authority certificate for server authentication when it uses a PEAP, EAP-TLS, or EAP-TTLS authentication method to connect to a Wi-Fi network.</p> <p>If you change this setting to Yes, a root certificate is not required for the PEAP, EAP-TLS, or EAP-TTLS authentication method.</p>
Possible values	<ul style="list-style-type: none"> • Yes • No
Default value	<ul style="list-style-type: none"> • No
Minimum requirements	<ul style="list-style-type: none"> • BlackBerry Device Software 5.0

Wi-Fi Domain Suffix configuration setting

Description	<p>This setting specifies the suffix for the internal domain name in FQDN format.</p>
Related settings	<p>The Wi-Fi DHCP Configuration configuration setting affects this configuration setting. Configure this setting only if you change the Wi-Fi DHCP Configuration configuration setting to No to make DHCP unavailable.</p>
Default value	<ul style="list-style-type: none"> • Null value
Minimum requirements	<ul style="list-style-type: none"> • BlackBerry Device Software 4.5

Wi-Fi EAP-FAST Provisioning method configuration setting

Description	<p>This setting specifies the type of provisioning method that a BlackBerry device can use when it authenticates with a Wi-Fi network using EAP-FAST authentication with PAC.</p> <p>If you want the server to authenticate the device using the user name and password for the user account and a root certificate when the device connects for the first time, you can select the Authenticated option. The device does not connect to the server if the server does not provide a root certificate to the device.</p> <p>If you want the server to authenticate the device using the user name and password for the user account without server authentication, you can select the Anonymous option.</p>
--------------------	---

	If you want the server to authenticate the device using the user name and password for the user account, and you want the settings on the server to determine if server authentication must occur, you can select the Both option. If the server provides a root certificate, the device verifies the server using the selected root certificate. If the server does not present a root certificate, the device does not perform server authentication.
Possible values	<ul style="list-style-type: none"> • Anonymous • Authenticated • Both
Default value	<ul style="list-style-type: none"> • Anonymous
Minimum requirements	<ul style="list-style-type: none"> • BlackBerry Device Software 5.0

Wi-Fi Enable Authentication Page configuration setting

Description	This setting specifies whether the Wi-Fi Login browser is available on a BlackBerry device. Change this setting to Yes to permit a BlackBerry device user to log in to a captive portal using the device.
Possible values	<ul style="list-style-type: none"> • Yes • No
Default value	<ul style="list-style-type: none"> • No
Minimum requirements	<ul style="list-style-type: none"> • BlackBerry Device Software 4.5

Wi-Fi Hard Token Required configuration setting

Description	This setting specifies whether a BlackBerry device requires a hard token for authentication. Change this setting to Yes if the device requires a hard token (for example, RSA SecurID) as part of the password for authentication.
Possible values	<ul style="list-style-type: none"> • Yes • No
Default value	<ul style="list-style-type: none"> • No
Minimum requirements	<ul style="list-style-type: none"> • BlackBerry Device Software 4.5

Wi-Fi Inner Authentication Mode configuration setting

Description	This setting specifies the authentication mode that a BlackBerry device uses for tunneled EAP security.
--------------------	---

Possible values	<ul style="list-style-type: none"> • None • EAP-MSCHAPV2 • EAP-GTC • PAP • CHAP • MSCHAP • MSCHAPV2 • EAP-MD5
Default value	<ul style="list-style-type: none"> • None
Minimum requirements	<ul style="list-style-type: none"> • BlackBerry Device Software 4.5

Wi-Fi Internet Access Path configuration setting

Description	This setting specifies how a BlackBerry device must access the Internet for Wi-Fi profiles that you configure for your organization.
Possible values	<ul style="list-style-type: none"> • Access through Wi-Fi • Access through BlackBerry MDS Connection Service • Auto-select
Default value	<ul style="list-style-type: none"> • Auto-select
Minimum requirements	<ul style="list-style-type: none"> • BlackBerry 6

Wi-Fi IP Address configuration setting

Description	This setting specifies the IP address (for example, 10.0.0.1) that a BlackBerry device can use if DHCP on the device is turned off.
Related settings	The Wi-Fi DHCP Configuration configuration setting affects this configuration setting. The device uses this setting only if you change the Wi-Fi DHCP Configuration configuration setting to No.
Default value	<ul style="list-style-type: none"> • Null value
Minimum requirements	<ul style="list-style-type: none"> • BlackBerry Device Software 4.5

Wi-Fi Link Security configuration setting

Description	This setting specifies the authentication method that a BlackBerry device requires to access a Wi-Fi network.
--------------------	---

Possible values	<ul style="list-style-type: none"> • Open Wi-Fi security • WEP • PSK • EAP-PEAP • EAP-LEAP • ESP-TLS • EAP-FAST • EAP-TTLS • EAP-SIM • EAP-AKA
Default value	<ul style="list-style-type: none"> • Open Wi-Fi security
Minimum requirements	<ul style="list-style-type: none"> • BlackBerry Device Software 4.5

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

Description	<p>This setting specifies the minimum security level for a private key that an EAP authentication method uses with a client certificate.</p> <p>If you configure this setting to Medium security, a BlackBerry device prompts a BlackBerry device user only once for the key store password so that the device can retrieve the private key and encrypt email messages. After the device retrieves the private key, the device retrieves the private key again only after the user resets the device. The device caches the private key in memory but does not store it with the Wi-Fi profile.</p> <p>If you configure this setting to High security, the device always prompts the user for the key store password when it accesses the private key and encrypts email messages. The device does not store the unencrypted private key with the Wi-Fi profile.</p> <p>If you configure this setting to Low security, the device prompts the user only once for the key store password so that the device can retrieve the private key and encrypt email messages. The device stores the unencrypted private key with the Wi-Fi profile.</p>
Possible values	<ul style="list-style-type: none"> • Low security • High security • Medium security
Default value	<ul style="list-style-type: none"> • Low security
Minimum requirements	<ul style="list-style-type: none"> • BlackBerry Device Software 4.5

Wi-Fi Preshared Key configuration setting

Description	This setting specifies the PSK if you use PSK in your organization to authenticate to Wi-Fi networks.
Related settings	The Wi-Fi Link Security configuration setting affects this configuration setting. A BlackBerry device uses this setting only if you set the Wi-Fi Link Security configuration setting to PSK.
Default value	<ul style="list-style-type: none"> Null value
Minimum requirements	<ul style="list-style-type: none"> BlackBerry Device Software 4.5

Wi-Fi Primary DNS configuration setting

Description	This setting specifies the primary DNS in IP address format (for example, 10.0.0.1) that a BlackBerry device can use if DHCP on the device is turned off.
Related settings	The Wi-Fi DHCP Configuration configuration setting affects this configuration setting. The device uses this configuration setting only if you change the Wi-Fi DHCP Configuration configuration setting to No.
Default value	<ul style="list-style-type: none"> Null value
Minimum requirements	<ul style="list-style-type: none"> BlackBerry Device Software 4.5

Wi-Fi Profile Editability configuration setting

Description	<p>This setting specifies whether a BlackBerry device user can change the settings in the Wi-Fi profile on a BlackBerry device.</p> <p>If you change this setting to No editability, the user cannot change any settings in the Wi-Fi profile. If you change this setting to Credentials editability, the user can change only the user credentials in the Wi-Fi profile.</p>
Possible values	<ul style="list-style-type: none"> Full editability No editability Credentials editability
Default value	<ul style="list-style-type: none"> Full editability
Minimum requirements	<ul style="list-style-type: none"> BlackBerry Device Software 4.5

Wi-Fi Profile Visibility configuration setting

Description	This setting specifies whether a BlackBerry device user can view the settings in the Wi-Fi profile. If you configure this setting to Restricted visibility, the BlackBerry device displays only the profile name. When you configure this setting to Credentials visibility, the device displays only the profile name and login information for the user.
Possible values	<ul style="list-style-type: none"> • Full visibility • Restricted visibility • Credentials visibility
Default value	<ul style="list-style-type: none"> • Full visibility
Minimum requirements	<ul style="list-style-type: none"> • BlackBerry Device Software 4.5

Wi-Fi Roaming Threshold configuration setting

Description	<p>This setting determines how often the Wi-Fi transceiver of a BlackBerry device scans for nearby wireless access points and roams to one of the access points if the signal quality is better than the signal of the current access point.</p> <p>If you configure this setting to Low, the device roams only when signal quality is very low. If you configure this setting to Medium, the device roams when the signal quality is medium to low. If you configure this setting to High, the device roams aggressively to access points with better signal strength. If you configure this setting to Auto, the device selects roaming thresholds automatically.</p>
Possible values	<ul style="list-style-type: none"> • Auto • Low • Medium • High
Default value	<ul style="list-style-type: none"> • Auto
Minimum requirements	<ul style="list-style-type: none"> • BlackBerry Device Software 4.5

Wi-Fi Secondary DNS configuration setting

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

Default value	<ul style="list-style-type: none"> Null value
Minimum requirements	<ul style="list-style-type: none"> BlackBerry Device Software 4.5

Wi-Fi Server SAN configuration setting

Description	This setting specifies a SAN field for the server certificate. If you do not specify a SAN field for the server certificate, a BlackBerry device accepts any valid server certificate.
Default value	<ul style="list-style-type: none"> Null value
Minimum requirements	<ul style="list-style-type: none"> BlackBerry Device Software 4.5

Wi-Fi Server Subject configuration setting

Description	This setting specifies the Subject field for the server certificate. If you do not specify the Subject field for a server certificate, a BlackBerry device accepts any valid server certificate.
Default value	<ul style="list-style-type: none"> Null value
Minimum requirements	<ul style="list-style-type: none"> BlackBerry Device Software 4.5

Wi-Fi SSID configuration setting

Description	This setting specifies the network name of a Wi-Fi network and its wireless access points. The SSID is case-sensitive and limited to 32 characters.
Default value	<ul style="list-style-type: none"> Null value
Minimum requirements	<ul style="list-style-type: none"> BlackBerry Device Software 4.5

Wi-Fi Subnet Mask configuration setting

Description	This setting specifies the subnet mask in IP address format (for example, 10.0.0.1) that a BlackBerry device can use if DHCP on the device is turned off.
Related settings	The Wi-Fi DHCP Configuration configuration setting affects this rule. The device uses this setting only if you change the Wi-Fi DHCP Configuration configuration setting to No.
Default value	<ul style="list-style-type: none"> Null value
Minimum requirements	<ul style="list-style-type: none"> BlackBerry Device Software 4.5

Wi-Fi Token Serial Number configuration setting

Description	If a BlackBerry device requires that a software token is part of the password for authentication, this setting specifies the serial number of the software token that is provided to the device.
Default value	<ul style="list-style-type: none"> Null value
Minimum requirements	<ul style="list-style-type: none"> BlackBerry Device Software 4.5

Wi-Fi User Name configuration setting

Description	This setting specifies the user name for PEAP authentication or LEAP authentication on a BlackBerry device. Configure this setting if you want to create a default value for all BlackBerry device users. If the user types a user name on the device manually, IT policy updates overwrite or delete the value that the user types. To retain the user-specified value on the device, verify that the updated Wi-Fi profile uses the same value as the Wi-Fi profile on the device.
Default value	<ul style="list-style-type: none"> Null value
Minimum requirements	<ul style="list-style-type: none"> BlackBerry Device Software 4.5

Wi-Fi User Password configuration setting

Description	This setting specifies the password for PEAP authentication or LEAP authentication on a BlackBerry device. Configure this setting if you want to create a default value for all BlackBerry device users. If the user types a password on the device manually, IT policy updates overwrite or delete the value that the user types. To retain the user-specified value on the device, verify that the updated Wi-Fi profile uses the same value as the Wi-Fi profile on the device.
Default value	<ul style="list-style-type: none"> Null value
Minimum requirements	<ul style="list-style-type: none"> BlackBerry Device Software 4.5

Wi-Fi WEP Key 1 configuration setting

Description	This setting specifies the password for WEP key 1 using the format xx:xx:xx:xx:xx. This configuration setting supports 5 or 13 pairs of hexadecimal digits (0 to 9 and A to F) that you separate with a colon (:). For example, AB:CD:EF:01:23 or AB:CD:EF:01:23:45:67:89:AB:CD:EF:01:23.
Default value	<ul style="list-style-type: none"> Null value

Minimum requirements	<ul style="list-style-type: none"> BlackBerry Device Software 4.5
-----------------------------	--

Wi-Fi WEP Key 2 configuration setting

Description	This setting specifies the password for WEP key 2 using the format <code>xx:xx:xx:xx:xx</code> . This configuration setting supports 5 or 13 pairs of hexadecimal digits (0 to 9 and A to F) that you separate with a colon (:). For example, <code>AB:CD:EF:01:23</code> or <code>AB:CD:EF:01:23:45:67:89:AB:CD:EF:01:23</code> .
Default value	<ul style="list-style-type: none"> Null value
Minimum requirements	<ul style="list-style-type: none"> BlackBerry Device Software 4.5

Wi-Fi WEP Key 3 configuration setting

Description	This setting specifies the password for WEP key 3 using the format <code>xx:xx:xx:xx:xx</code> . This configuration setting supports 5 or 13 pairs of hexadecimal digits (0 to 9 and A to F) that you separate with a colon (:). For example, <code>AB:CD:EF:01:23</code> or <code>AB:CD:EF:01:23:45:67:89:AB:CD:EF:01:23</code> .
Default value	<ul style="list-style-type: none"> Null value
Minimum requirements	<ul style="list-style-type: none"> BlackBerry Device Software 4.5

Wi-Fi WEP Key 4 configuration setting

Description	This setting specifies the password for WEP key 4 using the format <code>xx:xx:xx:xx:xx</code> . This configuration setting supports 5 or 13 pairs of hexadecimal digits (0 to 9 and A to F) that you separate with a colon (:). For example, <code>AB:CD:EF:01:23</code> or <code>AB:CD:EF:01:23:45:67:89:AB:CD:EF:01:23</code> .
Default value	<ul style="list-style-type: none"> Null value
Minimum requirements	<ul style="list-style-type: none"> BlackBerry Device Software 4.5

Examples of security goals

Requiring the use of a password on a device

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

Preventing the unauthorized use of a device

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

Glossary

5

AES

Advanced Encryption Standard

BlackBerry MDS

BlackBerry Mobile Data System

CHAP

Challenge Handshake Authentication Protocol

DES

Data Encryption Standard

DH

Diffie-Hellman

DHCP

Dynamic Host Configuration Protocol

DNS

Domain Name System

DSA

Digital Signature Algorithm

EAP

Extensible Authentication Protocol

EAP-AKA

Extensible Authentication Protocol Authentication and Key Agreement

EAP-FAST

Extensible Authentication Protocol Flexible Authentication via Secure Tunneling

EAP-GTC

Extensible Authentication Protocol Generic Token Card

EAP-LEAP

Extensible Authentication Protocol Lightweight Extensible Authentication Protocol

EAP-PEAP

Extensible Authentication Protocol Protected Extensible Authentication Protocol

EAP-SIM

Extensible Authentication Protocol Subscriber Identity Module

EAP-TLS

Extensible Authentication Protocol Transport Layer Security

EAP-TTLS

Extensible Authentication Protocol Tunneled Transport Layer Security

ECC

Elliptic Curve Cryptography

FQDN

fully qualified domain name

IKE

Internet Key Exchange

IP

Internet Protocol

MMS

Multimedia Messaging Service

PAC

Protected Access Credential

PAP

Password Authentication Protocol

PEAP

Protected Extensible Authentication Protocol

PFS

Perfect Forward Secrecy

PIM

personal information management

PKI

Public Key Infrastructure

PSK

pre-shared key

SMS

Short Message Service

SSID

service set identifier

USB

Universal Serial Bus

VPN

virtual private network

WEP

Wired Equivalent Privacy

Provide feedback

6

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

Legal notice

7

©2012 Research In Motion Limited. All rights reserved. BlackBerry®, RIM®, Research In Motion®, and related trademarks, names, and logos are the property of Research In Motion Limited and are registered and/or used in the U.S. and countries around the world.

Bluetooth is a trademark of Bluetooth SIG. Cisco is a trademark of Cisco Systems, Inc. IrDA is a trademark of Infrared Data Association. NetScreen is a trademark of Juniper Networks, Inc. Nortel Networks is a trademark of Nortel Networks Limited. Roxio is a trademark of Sonic Solutions. RSA and RSA SecurID are trademarks of RSA Security. Java and JavaScript are trademarks of Oracle America, Inc. Wi-Fi is a trademark of the Wi-Fi Alliance. All other trademarks are the property of their respective owners.

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

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

EXCEPT TO THE EXTENT SPECIFICALLY PROHIBITED BY APPLICABLE LAW IN YOUR JURISDICTION, ALL CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS, OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS OR WARRANTIES OF DURABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE, MERCHANTABILITY, 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