Guía de referencia de políticas

BlackBerry Enterprise Server Express

Versión: 5.0
Service Pack: 4

BlackBerry®

Publicado: 2012-10-29
SWD-20121029114457124

Contenido

1 Recursos relacionados 10

2 Novedades de esta versión 11

Nueva opción de configuración 11

Nuevas reglas de políticas de control de aplicaciones 11

3 Políticas de TI 12

Política de TI predeterminada 12

Valores predeterminados para las reglas de políticas de TI 12

4 Reglas de políticas de TI 18

Grupo de políticas de Sólo dispositivo 18

Regla de política de TI Permitir la mensajería "punto a punto" 18

Regla de política de TI Permitir SMS 18

Regla de política de TI Activar el tiempo de espera a largo plazo 19

Regla de política de TI Activar configuración WAP 20

Regla de política de TI Tiempo máximo de validez de la contraseña 20

Regla de política de TI Tiempo de espera de seguridad máximo 21

Regla de política de TI Longitud mínima de la contraseña 21

Regla de política de TI Comprobaciones de patrones de contraseña 22

Regla de política de TI Contraseña necesaria 23

Regla de política de TI El usuario puede modificar el tiempo de espera 23

Regla de política de TI El usuario puede desactivar la contraseña 24

Grupo de políticas globales 24

Regla de política de TI Permitir navegador 24

Regla de política de TI Permitir teléfono 25

Grupo de políticas de BlackBerry App World 25

Regla de política de TI Activar facturación del proveedor de servicios inalámbricos 25

Grupo de políticas de Bluetooth 26

Regla de política de TI Bluetooth 26

Regla de política de TI Desactivar el desvío inalámbrico 27

Grupo de políticas del navegador 27

Regla de política de TI Desactivar JavaScript en el navegador 28

Regla de política de TI Dominios del navegador MDS 28

Grupo de políticas de cámara 29

Regla de política de TI Desactivar cámara de fotos 29

Regla de política de TI Desactivar videocámara 29

Grupo de políticas comunes 30

Regla de política de TI Desactivar MMS 30
Regla de política de TI Desactivar la grabación de notas de voz 30
Grupo de políticas de mensajería de correo electrónico 31
Regla de política de TI Confirmar descarga de imagen externa 31
Regla de política de TI Desactivación de la descarga manual de imágenes externas 32
Regla de política de TI Desactivar reenviar y responder a mensajes de cifrado nativo de Lotus Notes 32
Regla de política de TI Desactivar el correo electrónico con contenido multimedia 33
Regla de política de TI Tamaño máximo de los archivos adjuntos originales MFH 33
Regla de política de TI Tamaño máximo total de los archivos adjuntos originales MFH 34
Regla de política de TI Tamaño máximo de los archivos adjuntos originales MTH 35
Regla de política de TI Tiempo de permanencia de la contraseña de cifrado original de Lotus Notes 35
Regla de política de TI Requerir cifrado original de Lotus Notes para mensajes salientes 36
Grupo de políticas de contraseña 37
Regla de política de TI Contraseñas prohibidas 37
Regla de política de TI Historial máximo de contraseñas 37
Regla de política de TI Tiempo periódico de búsqueda 38
Regla de política de TI Definir los intentos máximos de contraseña 39
Regla de política de TI Definir el tiempo de espera de contraseña 39
Regla de política de TI Suprimir el eco de la contraseña 40
Grupo de políticas de dispositivos personales 41
Regla de política de TI Desactivar el reenvío de contenido de trabajo mediante canales personales 41
Regla de política de TI Permitir la separación del contenido de trabajo 41
Regla de política de TI Requerir recursos de trabajo para realizar actividades de trabajo 42
Regla de política de TI Dominios de trabajo 43
Grupo de políticas de sincronización de la gestión PIM 44
Regla de política de TI Desactivar toda la sincronización inalámbrica 44
Grupo de políticas de aplicación PGP 45
Regla de política de TI Cifrados de contenido PGP permitido 45
Regla de política de TI Modo de archivo adjunto cifrado permitido de PGP 46
Regla de política de TI Tipos de cifrado PGP permitidos 46
Regla de política de TI PGP fuerza la firma digital 47
Regla de política de TI PGP fuerza los mensajes cifrados 48
Regla de política de TI Longitud mínima de la clave DSA fuerte PGP 48
Regla de política de TI Longitud mínima de la clave DSA fuerte PGP 49
Regla de política de TI Longitud mínima de la clave RSA fuerte PGP 50
Regla de política de TI Modo mensaje completo y envío PGP 50
Regla de política de TI Método de inscripción universal en PGP 51
Regla de política de TI Tiempo de permanencia en la caché de la política universal PGP 52
Regla de política de TI Dirección de PGP Universal Server 52
Grupo de políticas de aplicaciones de valor añadido de RIM 53

Regla de política de TI Desactivar el acceso a los datos del organizador para aplicaciones de redes sociales 53
Grupo de políticas de seguridad 54
Regla de política de TI Permitir conexiones externas 54
Regla de política de TI Permitir el restablecimiento del temporizador de inactividad 54
Regla de política de TI Permitir conexiones en ambos sentidos 55
Regla de política de TI Permitir que aplicaciones de otros fabricantes usen el puerto serie 55
Regla de política de TI Intensidad de protección de contenido 56
Regla de política de TI Desactivar 3DES Transport Crypto 57
Regla de política de TI Desactivar la memoria externa 57
Regla de política de TI Desactivar GPS 58
Regla de política de TI Desactivar módem IP 58
Regla de política de TI Desactivar el almacenamiento masivo USB 59
Regla de política de TI Desactivar la descarga de aplicaciones de otros fabricantes 60
Regla de política de TI Cifrado en archivos multimedia de la memoria de dispositivo integrada 61
Regla de política de TI Nivel de cifrado del sistema de archivos externo 61
Regla de política de TI Imponer bloqueo si el dispositivo está en la funda 62
Regla de política de TI Patrón de la contraseña necesaria 63
Regla de política de TI Restablecer valores predeterminados de serie al borrar 64
Regla de política de TI Algoritmos hash del archivo Cod del transcodificador de seguridad 64
Grupo de políticas de aplicación S/MIME 65
Regla de política de TI Dirección de correo electrónico del servidor de mensajería de confianza (EMS) 65
Regla de política de TI Cifrados de contenido S/MIME permitido 66
Regla de política de TI S/MIME Allowed Encrypted Attachment Mode 67
Regla de política de TI Tipos de cifrado S/MIME permitidos 67
Regla de política de TI S/MIME fuerza la firma digital 68
Regla de política de TI S/MIME fuerza los mensajes cifrados 69
Regla de política de TI Longitud mínima de la clave ECC fuerte S/MIME 69
Regla de política de TI Longitud mínima de la clave DSA fuerte S/MIME 70
Regla de política de TI Longitud mínima de la clave ECC fuerte S/MIME 71
Regla de política de TI Longitud mínima de la clave RSA fuerte S/MIME 71
Regla de política de TI Modo mensaje completo y envío S/MIME 72
Grupo de políticas de la VPN 73
Regla de política de TI Nombre de usuario de VPN 73
Regla de política de TI Contraseña de usuario de VPN 73
Grupo de políticas de Wi-Fi 74
Regla de política de TI Desactivar Wi-Fi 74
Grupo de políticas Actualizaciones de software con cable 74
Regla de política de TI Permitir la carga de software basado en Web 75
Regla de política de TI Copia de seguridad de servicios criptográficos 75
Grupo de políticas de actualizaciones inalámbricas de software 76

Regla de política de TI Desactivar la descarga de revisiones a través de WAN en itinerancia ... 76
5 Ajustes de configuración ... 77
Opciones de configuración de perfiles Wi-Fi ... 77
Configuración de la autoridad de certificación asociada ... 77
Opción Perfil VPN asociado ... 77
Opción de configuración Permitir la comunicación entre puntos de acceso Wi-Fi ... 78
Opción de configuración Permitir cambios de Wi-Fi en el dispositivo ... 78
Opción de configuración Permitir guardar contraseña de Wi-Fi ... 79
Opción de configuración Tipo de banda Wi-Fi ... 79
Opción de configuración Modo de acceso Wi-Fi de BlackBerry Infrastructure Wi-Fi ... 80
Opción de configuración Gateway predeterminada de Wi-Fi ... 80
Ajuste de configuración ID de clave predeterminada de Wi-Fi ... 81
Opción de configuración Configuración del DHCP en Wi-Fi ... 81
Opción de configuración Desactivar validación de certificado de servidor para Wi-Fi ... 82
Opción de configuración Sufijo de dominio de Wi-Fi ... 82
Opción de configuración Método de abastecimiento mediante EAP-FAST a través de Wi-Fi ... 83
Opción de configuración Activar página de autenticación de Wi-Fi ... 83
Opción de configuración Identificador físico de Wi-Fi solicitado ... 84
Opción de configuración Modo de autenticación interna de Wi-Fi ... 84
Ajuste de configuración de Ruta de acceso Wi-Fi a Internet ... 85
Opción de configuración Dirección IP de Wi-Fi ... 85
Opción de configuración Seguridad de Vínculo Wi-Fi ... 86
Opción de configuración Nivel de seguridad mínimo de la clave de cifrado del certificado EAP-TLS de Wi-Fi ... 86
Opción de configuración Clave Wi-Fi compartida previamente ... 87
Opción de configuración DNS principal de Wi-Fi ... 88
Opción de configuración Editabilidad del perfil Wi-Fi ... 88
Opción de configuración Visibilidad de perfil Wi-Fi ... 89
Opción de configuración Umbral de roaming de Wi-Fi ... 89
Opción de configuración DNS secundario de Wi-Fi ... 90
Opción de configuración SAN del servidor de Wi-Fi ... 90
Opción de configuración de Asunto del servidor de Wi-Fi ... 90
Opción de configuración SSID de Wi-Fi ... 91
Opción Máscara de subred de Wi-Fi ... 91
Opción de configuración Número de serie del identificador de Wi-Fi ... 91
Opción de configuración Nombre de usuario de Wi-Fi ... 92
Opción de configuración Contraseña de usuario de Wi-Fi ... 92
Opción de configuración Clave 1 WEP de Wi-Fi ... 93
Opción de configuración Clave 2 WEP de Wi-Fi ... 93
Opción de configuración Clave 3 WEP de Wi-Fi ... 93
Opción de configuración Clave 4 WEP de Wi-Fi ... 94

Configuración para perfiles de VPN 94
Configuración de la autoridad de certificación asociada 94
Configuración Activar VPN 95
Configuración Modo de división de túnel 95
Configuración Suprimir el título de VPN 95
Configuración Uso de los certificados Xauth de la VPN 96
Configuración Permitir cambios de VPN en el dispositivo 96
Configuración Permitir guardar contraseña de VPN 97
Configuración Desactivar validación del certificado del servidor de VPN 97
Configuración del DNS en la VPN 98
Configuración Nombre de dominio de la VPN 98
Configuración Dirección de gateway de la VPN 99
Configuración Nombre del grupo de VPN 99
Configuración Contraseña del grupo de VPN 99
Configuración Identificador físico de VPN solicitado 99
Configuración Cifrado IKE de la VPN 100
Configuración Grupo de claves DH del cifrado IKE de la VPN 100
Configuración Hash del cifrado IKE de la VPN 101
Configuración Dirección IP de VPN 101
Opción de configuración Cifrado y hash IPSec de la VPN 102
Configuración Nivel mínimo de seguridad de la clave de cifrado del certificado de VPN 103
Configuración Mantener activo NAT de VPN 103
Configuración PFS de la VPN 104
Configuración DNS principal de la VPN 104
Configuración Visibilidad del perfil VPN 105
Configuración Editabilidad del perfil VPN 105
Configuración DNS secundario de la VPN 105
Configuración Dirección IP de subred 1 de la VPN 106
Configuración Máscara de subred 1 de la VPN 106
Configuración Dirección IP de subred 2 de la VPN 107
Configuración Máscara de subred 2 de la VPN 107
Configuración Dirección IP de subred 3 de la VPN 107
Configuración Máscara de subred 3 de la VPN 108
Configuración Máscara de subred de la VPN 108
Configuración Número de serie del identificador de VPN 108
Configuración Nombre de usuario de VPN 109
Configuración Contraseña de usuario de VPN 109
Configuración Tipo de proveedor de VPN 110
Configuración Tipo de Xauth de la VPN 111
6 Reglas de políticas de control de aplicaciones 112

Regla de política de control de la aplicación ¿Se permiten las conexiones de redes externas? ... 112
Regla de política de control de la aplicación ¿Se permiten las conexiones de redes internas? ... 113
Regla de política de control de la aplicación ¿Se permiten las conexiones locales? ... 114
Regla de política de control de la aplicación ¿Se puede modificar la configuración del dispositivo? ... 114
Regla de política de control de la aplicación ¿Se puede restablecer el contador de seguridad? ... 115
Regla de política de control de aplicaciones Mostrar información mientras bloqueado ... 116
Regla de política de control de la aplicación Disponibilidad ... 116
Regla de política de control de la aplicación ¿Se permite el acceso a la API de los filtros del navegador? ... 117
Regla de política de control de aplicaciones ¿Se permite el acceso a los datos corporativos? ... 118
Regla de política de control de la aplicación ¿Se permite el acceso a la API del correo electrónico? ... 118
Regla de política de control de la aplicación ¿Se permite el acceso a la API de inyección de eventos? ... 119
Regla de política de control de la aplicación ¿Se permite el acceso a la API de archivo? ... 120
Regla de política de control de la aplicación ¿Se permite el acceso a la API del GPS? ... 120
Regla de política de control de la aplicación ¿Se permite el acceso al almacén de claves del dispositivo? ... 121
Regla de política de control de la aplicación ¿Se permite el acceso a la API de comunicación entre procesos? ... 122
Regla de política de control de la aplicación ¿Se permite el acceso a la API multimedia? ... 122
Regla de política de control de la aplicación ¿Se permite el acceso a la API de gestión del módulo? ... 123
Regla de política de control de la aplicación ¿Se permite el acceso al protocolo Near Field Communication (NFC)? ... 124
Regla de política de control de la aplicación ¿Se permite el acceso a la API del PIM? ... 124
Regla de política de control de la aplicación ¿Se permite el acceso a la API del teléfono? ... 125
Regla de política de control de la aplicación ¿Se permite el acceso a la pantalla, el micrófono y las API de captura de vídeo? ... 126
Regla de política de control de la aplicación ¿Se permite el acceso al elemento seguro? ... 126
Regla de política de control de la aplicación ¿Se permite el acceso al perfil de puerto de serie para la API de Bluetooth? ... 127
Regla de política de control de la aplicación ¿Se permite el acceso a la API del autenticador del usuario? ... 128
Regla de política de control de la aplicación ¿Se permite el acceso a la API de Wi-Fi? ... 129
Regla de política de control de la aplicación ¿Se permite la seguridad de medios del almacén de claves? ... 129
Regla de política de control de aplicaciones ¿Se permite la gestión de conexiones? ... 130
Regla de política de control de aplicaciones ¿Se permite el control multimedia? ... 130
Regla de política de control de la aplicación ¿Se permiten los datos de tema? ... 131
Regla de política de control de la aplicación Lista de dominios del filtro del navegador ... 132
Regla de política de control de la aplicación Lista de dominios externos ... 132
Regla de política de control de la aplicación Lista de dominios internos ... 133

7 Ejemplos de objetivos de la política de seguridad ... 134

Requisito del uso de una contraseña en un dispositivo ... 134
Evitar el uso no autorizado de un dispositivo ... 135
Cifrar los datos en un dispositivo ... 135
Restringir la mensajería en un dispositivo ... 136
Definir las medidas para evitar las amenazas de virus y usuarios malintencionados ... 137
Limitar los recursos a los que una aplicación de terceros puede acceder en un dispositivo ... 137

Limitación del control del usuario sobre aplicaciones de terceros en dispositivos BlackBerry 138
Cómo evitar que las aplicaciones de valor añadido de RIM se ejecuten en dispositivos BlackBerry 139
8 Glosario 141
9 Aviso legal 143

Recursos relacionados

1

Para leer las siguientes guías o material adicional relacionado, visite www.blackberry.com/go/serverdocs.

Guía	Información
Novedades integradas en BlackBerry Enterprise Server Express Ficha de ayuda de 5.0 SP4	• Resumen de nuevas características
Guía de actualización de BlackBerry Enterprise Server Express	• Resumen de actualizaciones a las guías de administrador para BlackBerry Enterprise Server Express 5.0 SP4
Notas de la versión de BlackBerry Enterprise Server Express	• Descripción de problemas conocidos y posibles soluciones
Guía de instalación y configuración de BlackBerry Enterprise Server Express	• Requisitos del sistema • Instrucciones de instalación
Guía de actualización de BlackBerry Enterprise Server Express	• Requisitos del sistema • Instrucciones de actualización

Novedades de esta versión

2

Nueva opción de configuración

Tipo de perfil	Valor	BlackBerry Device Software (requisito mínimo)
VPN	Configuración de la autoridad del certificado asociada	5.0

Nuevas reglas de políticas de control de aplicaciones

Regla	BlackBerry Device Software (requisito mínimo)
¿Se permite el acceso al protocolo Near Field Communication (NFC)?	7.0
¿Se permite el acceso al elemento seguro?	7.0

Políticas de TI

3

Puede asignar políticas de TI a dispositivos BlackBerry para cumplir los requisitos de seguridad de su empresa y las necesidades de los usuarios de los dispositivos BlackBerry. Por ejemplo, puede crear una política de TI, configurar las reglas para cumplir los requisitos de seguridad, agregar usuarios a un grupo y asignar la política de TI al grupo.

Para obtener más información sobre cómo crear una política de TI, configurar reglas de política de TI y asignar una política de TI a un grupo o cuenta de usuario, consulte la *Guía de administración de BlackBerry Enterprise Server Express* .

Política de TI predeterminada

BlackBerry Enterprise Server Express incluye una política de TI predeterminada. Cuando instala , las reglas de política de TI de la política de TI predeterminada no contienen ningún valor. Si no especifica un valor para una regla de política de TI, se utilizará el valor predeterminado. Puede configurar y aplicar la política de TI predeterminada a cuentas de usuario o puede crear nuevas políticas de TI y asignarlas a cuentas de usuario para controlar los dispositivos BlackBerry en el entorno de su empresa.

Valores predeterminados para las reglas de políticas de TI

Grupo de políticas de IT	Regla de política de TI	Valor predeterminado
Sólo en dispositivo	Permitir la mensajería "punto a punto"	Sí
Sólo en dispositivo	Permitir SMS	Sí
Sólo en dispositivo	Activar el tiempo de espera a largo plazo	Sí
Sólo en dispositivo	Activar configuración WAP	Sí
Sólo en dispositivo	Tiempo máximo de validez de la contraseña	Valor nulo

Grupo de políticas de IT	Regla de política de TI	Valor predeterminado
Sólo en dispositivo	Tiempo de espera de seguridad máximo	Valor nulo
Sólo en dispositivo	Longitud mínima de la contraseña	Valor nulo
Sólo en dispositivo	Comprobaciones de patrones de contraseña	Sin restricciones
Sólo en dispositivo	Contraseña necesaria	No
Sólo en dispositivo	El usuario puede modificar el tiempo de espera	Sí
Sólo en dispositivo	El usuario puede desactivar la contraseña	Sí
Elementos globales	Permitir navegador	Sí
Elementos globales	Permitir teléfono	Sí
BlackBerry App World	Activar la facturación del proveedor de servicios inalámbricos	No
Bluetooth	Desactivar Bluetooth	No
Bluetooth	Desactivar el desvío inalámbrico	Sí
Navegador	Desactivar JavaScript en el navegador	No
Navegador	Dominios del navegador MDS	Valor nulo
Cámara	Desactivar cámara de fotos	No
Cámara	Desactivar cámara de vídeo	No
Común	Desactivar MMS	No
Común	Desactivar la grabación de notas de voz	No
Mensajería de correo electrónico	Confirmar la descarga de imágenes externas	No
Mensajería de correo electrónico	Desactivación de la descarga manual de imágenes externas	No
Mensajería de correo electrónico	Desactivar reenviar y responder a mensajes de cifrado nativo de Lotus Notes	No
Mensajería de correo electrónico	Desactivación del correo electrónico con contenido multimedia	No

Grupo de políticas de IT	Regla de política de TI	Valor predeterminado
Mensajería de correo electrónico	Tamaño máximo de los archivos adjuntos originales MFH	3.145.728 bytes (3 MB)
Mensajería de correo electrónico	Tamaño máximo total de los archivos adjuntos originales MFH	5 MB
Mensajería de correo electrónico	Tamaño máximo de los archivos adjuntos originales MTH	10.240 KB
Mensajería de correo electrónico	Tiempo de permanencia de la contraseña de cifrado original de Lotus Notes	-1
Mensajería de correo electrónico	Requerir cifrado original de Lotus Notes para mensajes salientes	No
Contraseña	Contraseñas prohibidas	Valor nulo
Contraseña	Historial máximo de contraseñas	0
Contraseña	Tiempo periódico de búsqueda	Sí (60 minutos)
Contraseña	Definir los intentos máximos de contraseña	10
Contraseña	Definir el tiempo de espera de contraseña	2 minutos (versiones de BlackBerry Device Software anteriores a 4.7) 30 minutos (BlackBerry Device Software 4.7 y posteriores)
Contraseña	Suprimir el eco de la contraseña	Sí
Dispositivos personales	Desactivar el reenvío de contenido de trabajo mediante canales personales	No
Dispositivos personales	Permitir la separación del contenido de trabajo	No
Dispositivos personales	Requerir recursos de trabajo para realizar actividades de trabajo	No
Dispositivos personales	Dominios de trabajo	Valor nulo

Grupo de políticas de IT	Regla de política de TI	Valor predeterminado
Sincronización de PIM	Desactivar toda la sincronización inalámbrica	No
Aplicación PGP	Cifrados de contenido PGP permitido	Utilice todos los algoritmos compatibles
Aplicación PGP	Modo de archivo adjunto cifrado permitido de PGP	Automático
Aplicación PGP	Tipos de cifrado PGP permitidos	Ambas
Aplicación PGP	PGP fuerza la firma digital	No
Aplicación PGP	PGP fuerza los mensajes cifrados	No
Aplicación PGP	Longitud mínima de la clave DH fuerte PGP	1024 bits
Aplicación PGP	Longitud mínima de la clave DSA fuerte PGP	1024 bits
Aplicación PGP	Longitud mínima de la clave RSA fuerte PGP	1024 bits
Aplicación PGP	Modo mensaje completo y envío PGP	Manual
Aplicación PGP	Método de inscripción universal en PGP	Inscripción basada en correo electrónico
Aplicación PGP	Tiempo de permanencia en la caché de la política universal PGP	24 horas
Aplicación PGP	Dirección del servidor universal PGP	Valor nulo
Aplicaciones RIM Value-Added	Desactivar el acceso a los datos del organizador para aplicaciones de redes sociales	Sí
Seguridad	Permitir conexiones externas	Sí
Seguridad	Permitir el restablecimiento del temporizador de inactividad	No
Seguridad	Permitir conexiones en ambos sentidos	No
Seguridad	Permitir que aplicaciones de otros fabricantes usen el puerto serie	Sí
Seguridad	Intensidad de protección de contenido	Valor nulo
Seguridad	Desactivar 3DES Transport Crypto	No

Grupo de políticas de IT	Regla de política de TI	Valor predeterminado
Seguridad	Desactivar la memoria externa	No
Seguridad	Desactivar GPS	No
Seguridad	Desactivar módem IP	No
Seguridad	Desactivar el almacenamiento masivo USB	No
Seguridad	Desactivar la descarga de aplicaciones de otros fabricantes	No
Seguridad	Cifrado en archivos multimedia de la memoria de dispositivo integrada	Permitido
Seguridad	Nivel de cifrado del sistema de archivos externo	No necesario
Seguridad	Forzar bloqueo si en la funda	No
Seguridad	Patrón de la contraseña necesaria	Valor nulo
Seguridad	Restablecer los valores predeterminados de serie al borrar	No
Seguridad	Algoritmos hash del archivo Cod del transcodificador de seguridad	Valor nulo
Aplicación S/MIME	Dirección de correo electrónico del servidor de mensajería de confianza	Valor nulo
Aplicación S/MIME	Cifrados de contenido S/MIME permitido	Utilice todos los algoritmos compatibles
Aplicación S/MIME	Modo de archivo adjunto cifrado permitido de S/MIME	Automático
Aplicación S/MIME	Tipos de cifrado S/MIME permitidos	Ambas
Aplicación S/MIME	S/MIME fuerza la firma digital	No
Aplicación S/MIME	S/MIME fuerza los mensajes cifrados	No
Aplicación S/MIME	Longitud mínima de la clave DH fuerte S/MIME	1024 bits
Aplicación S/MIME	Longitud mínima de la clave DSA fuerte S/MIME	1024 bits
Aplicación S/MIME	Longitud mínima de la clave ECC fuerte S/MIME	163 bits
Aplicación S/MIME	Longitud mínima de la clave RSA fuerte S/MIME	1024 bits

Grupo de políticas de IT	Regla de política de TI	Valor predeterminado
Aplicación S/MIME	Modo mensaje completo y envío S/MIME	Manual
VPN	Nombre de usuario de VPN	Valor nulo
VPN	Contraseña de usuario de VPN	Valor nulo
Wi-Fi	Desactivar Wi-Fi	No
Actualizaciones del software con cable	Permitir la carga de software basado en Web	No
Actualizaciones del software con cable	Copia de seguridad de servicios criptográficos	Sí
Actualizaciones inalámbricas de software	Desactivar la descarga de revisiones a través de WAN en itinerancia	No

Reglas de políticas de TI

4

BlackBerry Enterprise Server Express incluye reglas de políticas de TI que puede configurar para cumplir con los requisitos de seguridad de la empresa y las necesidades de los usuarios del dispositivo BlackBerry.

Grupo de políticas de Sólo dispositivo

Regla de política de TI Permitir la mensajería "punto a punto"

Descripción	Esta regla especifica si un usuario de dispositivo BlackBerry puede enviar mensajes PIN. Esta regla no impide al usuario recibir mensajes PIN.
Valores posibles	• Sí • No
Valor predeterminado	• Sí
Requisitos mínimos	• BlackBerry Device Software 3.6
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP2

Regla de política de TI Permitir SMS

Descripción	Esta regla especifica si un usuario del dispositivo BlackBerry puede enviar mensajes de texto SMS. Esta regla no impide al usuario recibir mensajes SMS.

	Esta regla no impide al usuario enviar y recibir mensajes MMS. Para impedir al usuario enviar y recibir mensajes MMS, puede utilizar la regla de política de TI Desactivar MMS.
Valores posibles	• Sí • No
Valor predeterminado	• Sí
Requisitos mínimos	• BlackBerry Device Software 3.6
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de TI Activar el tiempo de espera a largo plazo

Descripción	Esta regla especifica si el dispositivo BlackBerry se bloquea pasado un espacio de tiempo predefinido, independientemente de si el usuario del dispositivo BlackBerry utiliza el dispositivo.
Reglas relacionadas	La regla de política de TI Tiempo periódico de búsqueda afecta a esta regla. Utilice la regla de política de TI Tiempo periódico de búsqueda para acortar o ampliar el intervalo de tiempo de espera.
Valores posibles	• Sí • No
Valores predeterminados	• No en la política de TI predeterminada
Requisitos mínimos	• BlackBerry Device Software 3.6
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP2

Regla de política de TI Activar configuración WAP

Descripción	Esta regla especifica si se impide que un usuario de dispositivo BlackBerry pueda utilizar el navegador WAP en un dispositivo BlackBerry. Si desactiva el navegador WAP y el proveedor de servicios de red de su empresa utiliza el servicio WAP para la mensajería MMS, debe desactivar la capacidad de enviar y recibir mensajes MMS.
Valores posibles	• Sí • No
Valor predeterminado	• Sí
Requisitos mínimos	• BlackBerry Device Software 3.6
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP3

Regla de política de TI Tiempo máximo de validez de la contraseña

Descripción	Esta regla especifica el número de días antes de que una contraseña del dispositivo BlackBerry caduque y que el usuario de dispositivo BlackBerry deba establecer una nueva contraseña. Si configura esta regla en 0, la contraseña del dispositivo no caduca.
Reglas de política de TI relacionadas	La regla de política de TI Contraseña necesaria afecta a esta regla. Un dispositivo utiliza esta regla sólo si la regla de política de TI Contraseña necesaria se configura en Sí.
Valores posibles	• De 0 a 65.535 días
Valores predeterminados	• 0 días en la política de TI Predeterminada
Requisitos mínimos	• BlackBerry Device Software 3.6

Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de TI Tiempo de espera de seguridad máximo

Descripción	Esta regla especifica el tiempo máximo que un usuario de dispositivo BlackBerry puede establecer como valor de tiempo de espera de seguridad. El valor del tiempo de espera de seguridad es el número de minutos de inactividad antes de que se bloquee el dispositivo BlackBerry.
Reglas relacionadas	La regla de política de TI Contraseña necesaria afecta a esta regla. Un dispositivo utiliza esta regla sólo si la regla de política de Contraseña necesaria se configura en Sí. La regla de política de TI El usuario puede modificar el tiempo de espera afecta a esta regla. Un usuario puede especificar cualquier valor de tiempo de espera por debajo del valor máximo, a menos que la regla de política de TI El usuario puede modificar el tiempo de espera esté establecida en No.
Valores posibles	• De 10 a 480 minutos
Valores predeterminados	• Valor nulo en la política de TI predeterminada
Requisitos mínimos	• BlackBerry Device Software 3.6
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de TI Longitud mínima de la contraseña

Descripción	Esta regla especifica el número mínimo de caracteres requeridos para la contraseña de un dispositivo BlackBerry. Esta regla no controla el número máximo de caracteres para la contraseña. El número máximo es de 32 caracteres.

Reglas relacionadas	La regla de política de TI Contraseña necesaria afecta a esta regla. Un dispositivo utiliza esta regla sólo si la regla de política de TI Contraseña necesaria se configura en Sí.
Valores posibles	• De 4 a 14 caracteres
Valor predeterminado	• Valor nulo
Requisitos mínimos	• BlackBerry Device Software 3.6
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de TI Comprobaciones de patrones de contraseña

Descripción	Esta regla especifica si es necesario comprobar que los caracteres de una contraseña de dispositivo BlackBerry coinciden con un patrón específico. De forma predeterminada, el dispositivo evita que un usuario del dispositivo BlackBerry configure una contraseña que utilice una secuencia natural de caracteres o números. Si se introduce un símbolo en una secuencia natural, el dispositivo puede utilizar la contraseña.
Reglas relacionadas	La regla de política de TI Contraseña necesaria afecta a esta regla. Un dispositivo utiliza esta regla sólo si la regla de política de Contraseña necesaria se configura en Sí.
Valores posibles	• Al menos 1 carácter alfabético y 1 carácter numérico • Al menos 1 carácter alfabético, 1 carácter numérico y 1 carácter especial • Al menos 1 carácter alfabético en mayúscula, 1 carácter alfabético en minúscula, 1 carácter numérico y 1 carácter especial • Sin restricciones
Valores predeterminados	• Ninguna restricción en la política de TI Predeterminada
Requisitos mínimos	• BlackBerry Device Software 3.6

Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de TI Contraseña necesaria

Descripción	Esta regla especifica si un usuario de dispositivo BlackBerry debe configurar una contraseña en un dispositivo BlackBerry.
Valores posibles	• Sí • No
Valores predeterminados	• No en la política de TI predeterminada
Requisitos mínimos	• BlackBerry Device Software 3.6
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de TI El usuario puede modificar el tiempo de espera

Descripción	Esta regla especifica si un usuario de dispositivo BlackBerry puede omitir el valor de tiempo de espera de seguridad.
Valores posibles	• Sí • No
Valor predeterminado	• Sí
Requisitos mínimos	• BlackBerry Device Software 3.6
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de TI El usuario puede desactivar la contraseña

Descripción	Esta regla especifica si un usuario de dispositivo BlackBerry puede desactivar el requisito de una contraseña de seguridad en un dispositivo BlackBerry. Esta regla es obsoleta para BlackBerry Device Software 4.0 o posterior.
Reglas relacionadas	La regla de política de TI Contraseña necesaria afecta a esta regla. Un dispositivo utiliza esta regla sólo si la regla de política de TI Contraseña necesaria se configura en Sí.
Valores posibles	• Sí • No
Valores predeterminados	• Sí en la política de TI Predeterminada
Requisitos mínimos	• BlackBerry Device Software 3.6
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Grupo de políticas globales

Regla de política de TI Permitir navegador

Descripción	Esta regla especifica si se encuentra disponible BlackBerry Browser en un dispositivo BlackBerry. Esta regla no afecta a otros navegadores.
Valores posibles	• Sí • No

Valor predeterminado	• Sí
Requisitos mínimos	• BlackBerry Device Software 3.6
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP2

Regla de política de TI Permitir teléfono

Descripción	Esta regla especifica si el teléfono se encuentra disponible en un dispositivo BlackBerry.
Valores posibles	• Sí • No
Valor predeterminado	• Sí
Requisitos mínimos	• BlackBerry Device Software 3.6
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP2

Grupo de políticas de BlackBerry App World

Regla de política de TI Activar facturación del proveedor de servicios inalámbricos

Descripción	Esta regla especifica si un usuario del dispositivo BlackBerry puede comprar aplicaciones del escaparate BlackBerry App World siguiendo el plan de compras del proveedor de servicios inalámbricos de su empresa.

Ejemplo	Gestiona BlackBerry Enterprise Server Express en una agencia inmobiliaria. Muchos de los usuarios de dispositivos BlackBerry de la agencia han indicado varias aplicaciones en el escaparate BlackBerry App World que pueden ayudarles a buscar nuevas propiedades. Tiene la aprobación de dirección para permitir a los empleados que compren las aplicaciones mediante el plan de compras del proveedor de servicios inalámbricos de la agencia.
Valores posibles	• Sí • No
Valores predeterminados	• No
Requisitos mínimos	• BlackBerry Device Software 4.5
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP2

Grupo de políticas de Bluetooth

Para obtener más información sobre la seguridad de Bluetooth® en dispositivos BlackBerry, consulte *Descripción técnica general sobre seguridad de BlackBerry Enterprise Solution* y *Seguridad para los dispositivos BlackBerry con tecnología inalámbrica Bluetooth* .

Regla de política de TI Bluetooth

Descripción	Esta regla especifica si está desactivada la compatibilidad con la tecnología Bluetooth® en un dispositivo BlackBerry Si está activada la tecnología Bluetooth cuando un dispositivo recibe esta regla, el usuario debe restablecer el dispositivo BlackBerry para que el cambio surta efecto.
Valores posibles	• Sí • No
Valor predeterminado	• No

Requisitos mínimos	• BlackBerry Device Software 3.8
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de TI Desactivar el desvío inalámbrico

Descripción	Esta regla especifica si se debe evitar el desvío inalámbrico mediante tecnología Bluetooth® en un dispositivo BlackBerry.
Ejemplo	Muchos empleados tienen ordenadores con tecnología Bluetooth. Bluetooth La tecnología permite a los usuarios conectar sus ordenadores a dispositivos que admiten Bluetooth mediante una conexión inalámbrica Bluetooth. Puede permitir que los usuarios sincronicen sus dispositivos con BlackBerry Desktop Software mediante una conexión Bluetooth en vez de usar la red del proveedor de servicios inalámbricos de su empresa. Puede permitir las conexiones Bluetooth para contribuir a reducir el uso de la red inalámbrica en el entorno de su empresa.
Valores posibles	• Sí • No
Valor predeterminado	• Sí
Requisitos mínimos	• BlackBerry Device Software 4.1
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP3

Grupo de políticas del navegador

Las reglas del grupo de políticas Navegador se aplican a todas las configuraciones del navegador en el dispositivo BlackBerry.

Regla de política de TI Desactivar JavaScript en el navegador

Descripción	Esta regla especifica si se permite la ejecución de código JavaScript en un dispositivo BlackBerry.
Ejemplo	Algunos usuarios de dispositivos BlackBerry informan que BlackBerry Browser es lento al navegar por sitios Web específicos. Los sitios Web pueden usar JavaScript, un lenguaje de secuencias de comandos para una amplia gama de funciones, incluidas ventanas emergentes, validación de entrada de usuario o creación de una interfaz dinámica. Puede utilizar esta regla para evitar que los dispositivos procesen JavaScript. Esta regla desactiva la funcionalidad JavaScript en sitios Web pero quizás puede acelerar la experiencia de navegación.
Valores posibles	• Sí • No
Valor predeterminado	• No
Requisitos mínimos	• BlackBerry Device Software 4.0
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP2

Regla de política de TI Dominios del navegador MDS

Descripción	Esta regla especifica una lista de direcciones Web que un dispositivo BlackBerry debe recuperar mediante BlackBerry Browser y BlackBerry MDS Connection Service. Debe separar las distintas direcciones Web con una coma (,). Si desea permitir a BlackBerry Browser recuperar subdominios de una dirección Web, coloque un punto como prefijo del dominio (.). Por ejemplo, puede escribir ".ejemplo.com" para permitir que BlackBerry Browser recupere todos los subdominios de ejemplo.com (como, por ejemplo, correo.ejemplo.com, www.ejemplo.com).
Valor predeterminado	• Valor nulo
Requisitos mínimos	• BlackBerry Device Software 4.2

Introducción a las reglas	• BlackBerry Enterprise Server Express para Microsoft Exchange 5.0 SP2 MR1 • BlackBerry Enterprise Server Express para IBM Lotus Domino 5.0 SP2

Grupo de políticas de cámara

Regla de política de TI Desactivar cámara de fotos

Descripción	Esta regla especifica si la cámara de un dispositivo BlackBerry está activada.
Valores posibles	• Sí • No
Valor predeterminado	• No
Requisitos mínimos	• BlackBerry Device Software 4.2
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de TI Desactivar videocámara

Descripción	Esta regla especifica si está activada la cámara de vídeo del dispositivo BlackBerry.
Valores posibles	• Sí • No
Valor predeterminado	• No
Requisitos mínimos	• BlackBerry Device Software 4.3

Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Grupo de políticas comunes

Regla de política de TI Desactivar MMS

Descripción	Esta regla especifica si un usuario del dispositivo BlackBerry puede enviar y recibir mensajes MMS. Para obtener más información, consulte el folleto *Descripción técnica general sobre seguridad de BlackBerry Enterprise Solution* .
Valores posibles	• Sí • No
Valor predeterminado	• No
Requisitos mínimos	• BlackBerry Device Software 4.0.2
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de TI Desactivar la grabación de notas de voz

Descripción	Esta regla especifica si la aplicación Grabadora de notas de voz está disponible en un dispositivo BlackBerry.
Valores posibles	• Sí • No

Valor predeterminado	• No
Requisitos mínimos	• BlackBerry Device Software 4.3
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP2

Grupo de políticas de mensajería de correo electrónico

Las reglas del grupo de políticas Mensajería de correo electrónico controlan la reconciliación inalámbrica de mensajes y la visualización de archivos adjuntos.

Regla de política de TI Confirmar descarga de imagen externa

Descripción	Esta regla especifica si un dispositivo BlackBerry muestra un cuadro de diálogo de confirmación cuando un usuario de dispositivo BlackBerry hace clic en el enlace Obtener imágenes de un mensaje de correo electrónico en formato HTML. El mensaje que muestra el cuadro de diálogo de confirmación informa a los usuarios de que podrían exponer sus direcciones de correo electrónico si descargan una imagen de Internet.
Valores posibles	• Sí • No
Valor predeterminado	• No
Requisitos mínimos	• BlackBerry Device Software 5.0
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de TI Desactivación de la descarga manual de imágenes externas

Descripción	Esta regla especifica si un usuario de dispositivo BlackBerry puede solicitar manualmente ver el contenido al que hace referencia una URL (como imágenes) incorporado en mensajes de correo electrónico.
Valores posibles	• Sí • No
Valor predeterminado	• No
Requisitos mínimos	• BlackBerry Device Software 4.5
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de TI Desactivar reenviar y responder a mensajes de cifrado nativo de Lotus Notes

Descripción	Esta regla especifica si se impide que un usuario de dispositivo BlackBerry reenvíe y responda a mensajes de correo electrónico cifrados de IBM Lotus Domino desde un dispositivo BlackBerry. De forma predeterminada, un usuario con compatibilidad para la lectura de mensajes de correo electrónico cifrados de IBM Lotus Domino puede reenviar o contestar a mensajes de correo electrónico cifrados recibidos, descifrados y descomprimidos en el dispositivo. BlackBerry Messaging Agent descifra los mensajes de correo electrónico antes de que un dispositivo envíe mensajes de correo electrónico al destinatario como texto sin formato. Para obtener más información sobre la lectura de mensajes de correo electrónico cifrados de IBM Lotus Domino en un dispositivo, consulte la *Descripción técnica general sobre seguridad de BlackBerry Enterprise Solution* .
Valores posibles	• Sí • No

Valor predeterminado	• No
Requisitos mínimos	• BlackBerry Device Software 4.2.1
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP3

Regla de política de TI Desactivar el correo electrónico con contenido multimedia

Descripción	Esta regla especifica si un dispositivo BlackBerry puede recibir mensajes de correo electrónico en formato HTML o de texto enriquecido (RTF).
Valores posibles	• Sí • No
Valor predeterminado	• No
Requisitos mínimos	• BlackBerry Device Software 4.5
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de TI Tamaño máximo de los archivos adjuntos originales MFH

Descripción	Esta regla especifica el tamaño máximo de un archivo adjunto que un usuario de dispositivo BlackBerry puede enviar desde un dispositivo BlackBerry. Esta regla se aplica a los archivos adjuntos que superen los 60 KB. Si configura esta regla en 0, el dispositivo no puede enviar ningún archivo adjunto que supere los 60 KB. El dispositivo puede enviar archivos adjuntos de un tamaño inferior a los 60 KB. El dispositivo comprime los archivos adjuntos que tengan un tamaño inferior a los 60 KB e incluye los archivos adjuntos en el cuerpo del mensaje de correo electrónico.

	Si cambia el valor del campo Tamaño máximo de carga de archivos adjuntos individuales (KB) o del campo Tamaño máximo de adjuntos cargados a 0, el dispositivo no puede cargar ningún archivo adjunto que supere los 60 KB.
Ejemplo	Muchos usuarios envían mensajes de correo electrónico que incluyen archivos adjuntos grandes a sus compañeros, lo que puede afectar al rendimiento de BlackBerry Enterprise Server Express. Puede limitar el tamaño de archivos adjuntos de mensajes que los usuarios pueden enviar desde dispositivos para controlar el tráfico de red.
Reglas relacionadas	En BlackBerry Enterprise Server Express 5.0 SP1 o posterior, esta regla interactúa con el campo Tamaño máximo de carga de archivos adjuntos individuales (KB) en BlackBerry Administration Service. Si configura este campo, BlackBerry Enterprise Server Express enviará los valores al dispositivo mediante libros de servicios. El dispositivo no puede enviar un archivo adjunto que exceda el tamaño que haya especificado en el campo.
Valores posibles	• De 0 a 3.145.728 bytes
Valor predeterminado	• 3.145.728 bytes
Requisitos mínimos	• BlackBerry Device Software 4.2
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de TI Tamaño máximo total de los archivos adjuntos originales MFH

Descripción	Esta regla especifica el tamaño total de todos los archivos adjuntos estándar que se pueden cargar desde un dispositivo BlackBerry.
Ejemplo	Muchos usuarios de dispositivos BlackBerry envían mensajes de correo electrónico que incluyen uno o varios archivos adjuntos grandes a sus compañeros, lo que puede afectar al rendimiento de BlackBerry Enterprise Server Express. Puede limitar el tamaño total de los archivos adjuntos de mensajes que los usuarios pueden enviar desde dispositivos para controlar el tráfico de red.
Valores posibles	• De 0 a 5.242.880 bytes
Valor predeterminado	• 5.242.880 bytes

Requisitos mínimos	• BlackBerry Device Software 4.2
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de TI Tamaño máximo de los archivos adjuntos originales MTH

Descripción	Esta regla especifica el tamaño total de un archivo adjunto que puede enviar un usuario del dispositivo BlackBerry desde un dispositivo BlackBerry. Configure esta regla en 0 para evitar que el usuario descargue archivos adjuntos en el dispositivo.
Ejemplo	Muchos usuarios de dispositivos BlackBerry descargan archivos adjuntos de mensajes en sus dispositivos. Al personal de TI le preocupa el uso de los recursos de red adicionales y el posible riesgo de seguridad que supone la descarga de archivos adjuntos porque es posible que el remitente no siempre sea un empleado de confianza. Puede impedir que los usuarios descarguen archivos adjuntos en sus dispositivos. Los usuarios pueden abrir y ver archivos adjuntos de mensajes.
Valor posible	• De 0 a 1.048.576 KB
Valor predeterminado	• 10.240 KB
Requisitos mínimos	• BlackBerry Device Software 4.5
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de TI Tiempo de permanencia de la contraseña de cifrado original de Lotus Notes

Descripción	Esta regla especifica el tiempo máximo que un dispositivo BlackBerry guarda la contraseña de .id de IBM Lotus Notes introducida por el usuario del dispositivo BlackBerry. Cambie esta regla a 0 para evitar que el dispositivo almacene la contraseña que el usuario escribe en el dispositivo.

Valores posibles	• De -1 a 32.767 minutos
Valor predeterminado	• -1
Requisitos mínimos	• BlackBerry Device Software 4.3
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP3

Regla de política de TI Requerir cifrado original de Lotus Notes para mensajes salientes

Descripción	Esta regla especifica si el usuario del dispositivo BlackBerry puede enviar los mensajes de correo electrónico cifrados mediante el cifrado de IBM Lotus Notes. Si es necesario, el dispositivo BlackBerry solicita al usuario las contraseñas de cifrado de IBM Lotus Notes. El dispositivo no realiza el cifrado de IBM Lotus Notes, sino que configura los mensajes de correo electrónico que el dispositivo envía para el cifrado de IBM Lotus Notes que lleva a cabo BlackBerry Enterprise Server Express. Esta regla no afecta a los mensajes de correo electrónico que el dispositivo envía a través de servicios de correo electrónico no compatibles con el cifrado de IBM Lotus Notes.
Valores posibles	• Sí • No
Valor predeterminado	• No
Requisitos mínimos	• BlackBerry Device Software 5.0
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP3

Grupo de políticas de contraseña

Un dispositivo BlackBerry solamente utiliza las reglas de política de TI del grupo de políticas de contraseña si, en Sólo en dispositivo, la regla de política de TI Contraseña necesaria se configura en Sí. Para obtener más información acerca del uso de contraseñas en dispositivos BlackBerry, consulte la *Descripción técnica general sobre seguridad de BlackBerry Enterprise Solution* .

Regla de política de TI Contraseñas prohibidas

Descripción	Esta regla especifica las contraseñas que no puede utilizar un usuario de dispositivo BlackBerry. Separe varias contraseñas con una coma (,). De forma predeterminada, un dispositivo BlackBerry impide que un usuario configure contraseñas que utilicen una secuencia natural de caracteres o números. El dispositivo también impide automáticamente la sustitución de letras. Por ejemplo, si incluye "password" en la lista de contraseñas prohibidas, los usuarios no pueden utilizar "p@ssw0rd", "pa$zword" o "password123" en el dispositivo.
Reglas relacionadas	La regla de política de TI Contraseña necesaria afecta a esta regla. El dispositivo utiliza esta regla sólo si la regla de política de TI Contraseña necesaria se configura en Sí.
Valor predeterminado	• Valor nulo
Requisitos mínimos	• BlackBerry Device Software 4.1
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de TI Historial máximo de contraseñas

Descripción	Esta regla especifica el número máximo de contraseñas anteriores con las que un dispositivo BlackBerry compara las nuevas contraseñas a fin de evitar que un usuario de dispositivo BlackBerry vuelva a utilizar las antiguas contraseñas.

Reglas relacionadas	La regla de política de TI Contraseña necesaria afecta a esta regla. El dispositivo utiliza esta regla sólo si la regla de política de TI Contraseña necesaria se configura en Sí.
Ejemplo	Observa que numerosos usuarios reutilizan contraseñas que habían usado anteriormente cuando se les pide crear una nueva contraseña para sus dispositivos. Desea que los usuarios creen contraseñas nuevas cada vez, a fin de reducir el riesgo de que alguien descubra la contraseña de un usuario. Establezca esta regla en 15 de modo que, cuando un usuario escriba una nueva contraseña, no pueda ser ninguna de las 15 anteriores que el usuario ha especificado.
Valores posibles	• De 0 a 15 contraseñas
Valores predeterminados	• 0
Requisitos mínimos	• BlackBerry Device Software 3.6
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de TI Tiempo periódico de búsqueda

Descripción	Esta regla especifica el intervalo de tiempo de espera de seguridad tras el cual un dispositivo BlackBerry se bloquea y pide al usuario de dispositivo BlackBerry que escriba una contraseña, independientemente de si el dispositivo estaba activo durante dicho intervalo.
Reglas relacionadas	La regla de política de TI Contraseña necesaria afecta a esta regla. El dispositivo utiliza esta regla sólo si la regla de política de TI Contraseña necesaria se configura en Sí. La regla de política de TI El usuario puede modificar el tiempo de espera afecta a esta regla. Cambie el valor de la regla de política de TI El usuario puede modificar el tiempo de espera a No para que un usuario no pueda cambiar la configuración de tiempo de espera en un dispositivo. La regla de política de TI Activar el tiempo de espera a largo plazo afecta a esta regla. De forma predeterminada, si cambia la regla de política de TI Activar el tiempo de espera a largo plazo a Sí, el intervalo de tiempo de espera de seguridad se activa y se establece en 60 minutos.
Valores posibles	• De 1 a 1440 minutos
Valor predeterminado	• 60 minutos

Requisitos mínimos	• BlackBerry Device Software 4.0
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP2

Regla de política de TI Definir los intentos máximos de contraseña

Descripción	Esta regla especifica el número de veces que un usuario del dispositivo BlackBerry puede intentar introducir contraseña antes de que el dispositivo BlackBerry borre todos los datos de la aplicación de forma permanente.
Reglas relacionadas	La regla de política de TI Contraseña necesaria afecta a esta regla. El dispositivo utiliza esta regla sólo si la regla de política de TI Contraseña necesaria se configura en Sí.
Valores posibles	• De 3 a 10
Valor predeterminado	• 10
Requisitos mínimos	• BlackBerry Device Software 3.6
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de TI Definir el tiempo de espera de contraseña

Descripción	Esta regla especifica el tiempo de inactividad que puede ocurrir antes de que el usuario del dispositivo BlackBerry escriba la contraseña para desbloquear el dispositivo BlackBerry. Esta regla define el valor predeterminado para el tiempo de espera de seguridad.
Reglas relacionadas	La regla de política de TI El usuario puede modificar el tiempo de espera afecta a esta regla. Si configura la regla de política de TI El usuario puede modificar el tiempo de espera en No, el dispositivo utilizará el tiempo de espera de seguridad que usted configure en esta regla.

Valores posibles	• De 0 a 60 minutos
Valor predeterminado	• 2 minutos para BlackBerry Device Software 4.6 y anterior • 30 minutos para BlackBerry Device Software 4.7 y posterior
Requisitos mínimos	• BlackBerry Device Software 3.6
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de TI Suprimir el eco de la contraseña

Descripción	Esta regla especifica si los caracteres que escribe el usuario del dispositivo BlackBerry en el cuadro de diálogo Contraseña aparecen en la pantalla del dispositivo BlackBerry una vez que el usuario escribe la contraseña de forma incorrecta un número específico de veces.
Reglas relacionadas	La regla de política de TI Contraseña necesaria afecta a esta regla. El dispositivo utiliza esta regla sólo si se configura una contraseña en el dispositivo. Para requerir una contraseña, configure la regla de política de TI Contraseña necesaria en Sí. La regla de política de TI Definir los intentos máximos de contraseña afecta a esta regla. Para especificar el número de veces que el usuario puede escribir la contraseña de forma incorrecta antes de que los caracteres aparezcan en la pantalla, configure la regla de política de TI Definir los intentos máximos de contraseña.
Valores posibles	• Sí • No
Valor predeterminado	• No
Requisitos mínimos	• BlackBerry Device Software 3.6
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Grupo de políticas de dispositivos personales

Regla de política de TI Desactivar el reenvío de contenido de trabajo mediante canales personales

Descripción	Esta regla especifica si un usuario del dispositivo BlackBerry puede enviar datos del trabajo a contactos mediante recursos personales (por ejemplo, mensajes de texto SMS, mensajes MMS o mensajes de correo electrónico de cuentas de correo electrónico personales).
Reglas relacionadas	La regla de política de TI Permitir la separación del contenido de trabajo afecta a esta regla. El dispositivo BlackBerry sólo utiliza esta regla si configura en Sí la regla de política de TI Permitir la separación del contenido de trabajo.
Valores posibles	• Sí • No
Valor predeterminado	• No
Requisitos mínimos	• BlackBerry 6
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP3

Regla de política de TI Permitir la separación del contenido de trabajo

Descripción	Esta regla especifica si un dispositivo BlackBerry distingue entre los datos del trabajo y los datos personales, y si sólo las aplicaciones autorizadas del dispositivo pueden acceder a los datos del trabajo. Si configura esta regla en Verdadero y el usuario del dispositivo BlackBerry intenta eliminar el

	libro de servicios de escritorio, el smartphone solicitará al usuario que elimine los datos de trabajo del smartphone.
Ejemplo	Su empresa gestiona información confidencial que no se puede compartir con fuentes externas. Todos los usuarios de dispositivos BlackBerry de su empresa tienen una aplicación personalizada en sus dispositivos que utilizan para realizar el seguimiento de la información de clientes y compartirla. Puede utilizar esta regla y la regla de política de control de aplicaciones "Se permite el acceso a la API de datos de la empresa" para conceder a la aplicación personalizada acceso al contenido de la red y para evitar que todas las demás aplicaciones de terceros del dispositivo accedan al contenido de la red, como mensajes de correo electrónico, información de contacto e información de calendario.
Reglas relacionadas	La regla de política de control de aplicaciones "Se permite el acceso a la API de datos de la empresa" afecta esta regla. La regla de política de control de aplicaciones "Se permite el acceso a la API de datos de la empresa" especifica si una aplicación de terceros o una aplicación complementaria tiene autorización para acceder a los datos de trabajo. Para que esta regla afecte a aplicaciones de terceros, debe configurar la regla de política de control de aplicaciones "Se permite el acceso a la API de datos de la empresa" en No permitido para aplicaciones de terceros.
Valores posibles	• Sí • No
Valor predeterminado	• No
Requisitos mínimos	• BlackBerry 6
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP3

Regla de política de TI Requerir recursos de trabajo para realizar actividades de trabajo

Descripción	Esta regla especifica si un dispositivo BlackBerry debe utilizar los recursos de trabajo (por ejemplo, cuentas de correo electrónico o calendarios de trabajo) cuando un usuario de dispositivo BlackBerry lleva a cabo una actividad del trabajo (por ejemplo, enviar un mensaje correo electrónico a un contacto del trabajo o programar una cita de trabajo).
Reglas relacionadas	La regla de política de TI Permitir la separación del contenido de trabajo afecta a esta regla. El dispositivo sólo utiliza esta regla si configura la regla de política de TI Permitir la separación del contenido de trabajo en Sí.

Valores posibles	• Sí • No
Valor predeterminado	• No
Requisitos mínimos	• BlackBerry 6
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP3

Regla de política de TI Dominios de trabajo

Descripción	Esta regla especifica una lista de recursos (por ejemplo, los nombres de dominio, los nombres de servidor y los dominios de correo electrónico) que un dispositivo BlackBerry identifica como recursos de trabajo. Si indica un dominio, todos los subdominios del dominio se incluyen automáticamente. Si indica varios recursos, separe los recursos con una coma (,), un punto y coma (;) o un espacio. Por ejemplo, si su empresa tiene varios dominios, escriba ejemplo.com, ejemplo.net, ejemplo.org. Si configura esta regla, el dispositivo avisa al usuario del dispositivo BlackBerry cuando un mensaje de correo electrónico incluye una dirección que no pertenece a un dominio de trabajo. El dispositivo resalta las direcciones de correo electrónico que no pertenecen al dominio de trabajo en amarillo. Si el usuario intenta reenviar un correo electrónico a una dirección que no pertenece al dominio de trabajo o incluye en una respuesta una dirección que no pertenece a dicho dominio, el dispositivo también mostrará un mensaje de aviso.
Valor predeterminado	• Valor nulo
Requisitos mínimos	• BlackBerry 6
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP3

Grupo de políticas de sincronización de la gestión PIM

Regla de política de TI Desactivar toda la sincronización inalámbrica

Descripción	Esta regla especifica si la sincronización inalámbrica de datos está desactivada. Configure esta regla en Sí para desactivar toda la sincronización inalámbrica de datos, excepto la reconciliación inalámbrica del correo electrónico. Esta regla evita las siguientes acciones: • Sincronización inalámbrica de las entradas de contactos, las entradas de calendario, los filtros de mensajes de correo electrónico, las tareas y las notas • Sincronización inalámbrica de toda la información de registro • Copia de seguridad inalámbrica de datos, incluidos los datos de configuración para dispositivos BlackBerry • Cargas masivas inalámbricas • Activación de dispositivos a través de la red inalámbrica
Valores posibles	• Sí • No
Valor predeterminado	• No
Requisitos mínimos	• BlackBerry Device Software 4.0

Grupo de políticas de aplicación PGP

Las reglas de política de TI del grupo de políticas de aplicación PGP se aplican a dispositivos BlackBerry que ejecutan PGP Support Package para smartphones BlackBerry. Para obtener más información sobre el uso de PGP Support Package para smartphones BlackBerry, consulte *Información general técnica de seguridad de PGP Support Package para dispositivos BlackBerry* .

Regla de política de TI Cifrados de contenido PGP permitido

Descripción	Esta regla especifica los algoritmos de cifrado que un dispositivo BlackBerry puede utilizar para cifrar mensajes protegidos PGP. Para mantener la compatibilidad con la mayoría de los clientes PGP, utilice el cifrado Triple DES y CAST. De forma predeterminada, un dispositivo está diseñado para cifrar los mensajes de correo electrónico mediante cifrado Triple DES cuando no conoce la capacidad de descifrado del destinatario.
Ejemplo	Su empresa ha implementado la tecnología PGP para proteger los mensajes de correo electrónico y otros datos electrónicos que los empleados envían y reciben. Instale PGP Support Package para smartphones BlackBerry en los dispositivos para permitir que los usuarios de dispositivos BlackBerry envíen y reciban correo electrónico PGP y mensajes PIN. Su empresa únicamente admite el uso de los estándares AES y Triple DES, por lo que usa esta regla para permitir que los dispositivos usen estos cifrados de contenido para cifrar los mensajes PGP.
Valores posibles	• AES (256 bits) • AES (192 bits) • AES (128 bits) • CAST (128 bits) • Triple DES
Requisitos mínimos	• PGP Support Package para smartphones BlackBerry 4.1 • BlackBerry Device Software 4.1
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP2

Regla de política de TI Modo de archivo adjunto cifrado permitido de PGP

Descripción	Esta regla especifica el modo de recuperar información de archivos adjuntos protegidos PGP en un dispositivo BlackBerry.
Ejemplo	Los estándares de seguridad de su empresa especifican que los usuarios sólo deben abrir los archivos adjuntos de mensajes cifrados con PGP en sus ordenadores en un entorno de trabajo de alta seguridad. Puede utilizar esta regla para evitar que los usuarios recuperen los archivos adjuntos cifrados con PGP en sus dispositivos.
Valores posibles	• Ninguno • Manual • Automático
Valor predeterminado	• Automático
Requisitos mínimos	• BlackBerry Device Software 4.5
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP2

Regla de política de TI Tipos de cifrado PGP permitidos

Descripción	Esta regla especifica los tipos de cifrado que un dispositivo BlackBerry puede utilizar con mensajes protegidos PGP.
Ejemplo	Su empresa gestiona información que exige un elevado nivel de seguridad. Puede usar esta regla para admitir tanto el cifrado PGP como el cifrado convencional para mensajes de correo electrónico que se envían desde los dispositivos y se reciben en ellos.
Valores posibles	• Sólo basados en claves PGP • Sólo convencionales • Ambas

Valor predeterminado	• Ambas
Requisitos mínimos	• PGP Support Package para smartphones BlackBerry 4.0 • BlackBerry Device Software 4.6
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP2

Regla de política de TI PGP fuerza la firma digital

Descripción	Esta regla especifica si un dispositivo BlackBerry firma digitalmente todos los mensajes protegidos PGP que envía. Si se aplica esta regla, podría anularse la configuración de la política de correo electrónico de PGP Universal Server.
Ejemplo	Su empresa ha implementado la tecnología PGP para proteger los mensajes de correo electrónico y otros datos electrónicos que los empleados envían y reciben. Instale PGP Support Package para smartphones BlackBerry en los dispositivos para permitir que los usuarios de dispositivos BlackBerry envíen y reciban correo electrónico PGP y mensajes PIN. Los estándares de seguridad de su empresa requieren que todos los mensajes de correo electrónico se deben firmar digitalmente. Las firmas digitales se usan para verificar que el mensaje lo ha enviado el usuario correcto. Puede utilizar esta regla para agregar firmas digitales a todos los mensajes PGP que se envían desde los dispositivos.
Valores posibles	• Sí • No
Valor predeterminado	• No
Requisitos mínimos	• PGP Support Package para smartphones BlackBerry 4.1 • BlackBerry Device Software 4.1
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP2

Regla de política de TI PGP fuerza los mensajes cifrados

Descripción	Esta regla especifica si un dispositivo BlackBerry cifra todos los mensajes protegidos PGP que envía. Si se aplica esta regla, podría anularse la configuración de la política de correo electrónico de PGP Universal Server.
Ejemplo	Su empresa ha implementado la tecnología PGP para proteger los mensajes de correo electrónico y otros datos electrónicos que los empleados envían y reciben. Instale PGP Support Package para smartphones BlackBerry en los dispositivos para permitir que los usuarios de dispositivos BlackBerry envíen y reciban correo electrónico PGP y mensajes PIN. Para cumplir los requisitos de su empresa a fin de obtener una comunicación móvil de alta seguridad, puede usar esta regla para que los dispositivos cifren todos los mensajes de correo electrónico que los usuarios reenvían o a los que responden mediante el cifrado PGP.
Valores posibles	• Sí • No
Valor predeterminado	• No
Requisitos mínimos	• PGP Support Package para smartphones BlackBerry 4.1 • BlackBerry Device Software 4.1
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP2

Regla de política de TI Longitud mínima de la clave DSA fuerte PGP

Descripción	Esta regla especifica el tamaño de clave Diffie-Hellman mínimo que se debe utilizar con los mensajes protegidos PGP.
Ejemplo	Los dispositivos BlackBerry usan claves públicas PGP y claves privadas PGP para cifrar y descifrar mensajes de correo electrónico. Las claves PGP pueden usar el algoritmo DH para el cifrado y

	descifrado. La longitud de la clave en bits es un factor importante para determinar la intensidad de la clave. Su empresa admite una longitud de clave mínima de 512 bits para las claves que usan el algoritmo DH, por lo que especifica 512 bits en esta regla para permitir que los dispositivos admitan claves PGP de esta longitud o superior.
Valores posibles	• De 512 a 4096 bits
Valor predeterminado	• 1024 bits
Requisitos mínimos	• PGP Support Package para smartphones BlackBerry 4.1 • BlackBerry Device Software 4.1
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP2

Regla de política de TI Longitud mínima de la clave DSA fuerte PGP

Descripción	Esta regla especifica el tamaño de clave DSA mínimo que se debe utilizar con los mensajes protegidos PGP. El intervalo permitido es de 512 a 1024 bits.
Ejemplo	Los dispositivos BlackBerry usan claves públicas PGP y claves privadas PGP para cifrar y descifrar mensajes de correo electrónico. Las claves PGP pueden usar el algoritmo DSA para el cifrado y descifrado. La longitud de la clave en bits es un factor importante para determinar la intensidad de la clave. Su empresa admite una longitud de clave mínima de 512 bits para las claves que usan el algoritmo DSA, por lo que especifica 512 bits en esta regla para permitir que los dispositivos admitan claves PGP de esta longitud o superior.
Valores posibles	• De 512 a 1024 bits
Valor predeterminado	• 1024 bits
Requisitos mínimos	• PGP Support Package para smartphones BlackBerry 4.1 • BlackBerry Device Software 4.1
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP2

Regla de política de TI Longitud mínima de la clave RSA fuerte PGP

Descripción	Esta regla especifica el tamaño de clave RSA mínimo que debe utilizarse con los mensajes protegidos PGP.
Ejemplo	Los dispositivos BlackBerry usan claves públicas PGP y claves privadas PGP para cifrar y descifrar mensajes de correo electrónico. Las claves PGP pueden usar el algoritmo RSA para el cifrado y descifrado. La longitud de la clave en bits es un factor importante para determinar la intensidad de la clave. Su empresa admite una longitud de clave mínima de 512 bits para las claves que usan el algoritmo RSA, por lo que especifica 512 bits en esta regla para permitir que los dispositivos admitan claves PGP de esta longitud o superior.
Valores posibles	• De 512 a 4096 bits
Valor predeterminado	• 1024 bits
Requisitos mínimos	• PGP Support Package para smartphones BlackBerry 4.1 • BlackBerry Device Software 4.1
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP2

Regla de política de TI Modo mensaje completo y envío PGP

Descripción	Esta regla especifica el modo que el dispositivo BlackBerry utiliza para recuperar el texto completo de un mensaje de correo electrónico cuando un usuario del dispositivo BlackBerry responda o reenvíe el mensaje de correo electrónico.
Ejemplo	De forma predeterminada, los usuarios de dispositivos BlackBerry deben solicitar el texto completo de los mensajes de correo electrónico a los que responden o reenvían como mensajes PGP desde sus dispositivos. Puede utilizar esta regla para que los dispositivos recuperen y muestren automáticamente el texto completo de los mensajes a los que responden los usuarios o reenvían como mensajes PGP.

Valores posibles	• Automático • Manual • Ninguno
Valor predeterminado	• Manual
Requisitos mínimos	• BlackBerry Device Software 5.0
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP2

Regla de política de TI Método de inscripción universal en PGP

Descripción	Esta regla especifica el método que debe utilizar el usuario de un dispositivo BlackBerry para inscribirse con PGP Universal Server en un dispositivo BlackBerry. El usuario debe enviar la información de inscripción a PGP Universal Server antes de que el usuario envíe y reciba mensajes protegidos PGP al dispositivo.
Ejemplo	Para admitir el cifrado PGP con PGP Universal Server, los usuarios de dispositivos BlackBerry deben inscribir los dispositivos con PGP Universal Server de su empresa. De forma predeterminada, la inscripción basada en correo electrónico se utiliza para inscribir los dispositivos con PGP Universal Server. Para cumplir los requisitos de seguridad de su empresa, puede utilizar esta regla para aplicar un método alternativo que requiera que los usuarios especifiquen su nombre de usuario y contraseña de dominio para inscribir sus dispositivos.
Valores posibles	• Inscripción con nombre de usuario/contraseña de dominio • Inscripción basada en correo electrónico
Valor predeterminado	• Inscripción basada en correo electrónico
Requisitos mínimos	• PGP Support Package para smartphones BlackBerry 4.1 • BlackBerry Device Software 4.1

Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP2

Regla de política de TI Tiempo de permanencia en la caché de la política universal PGP

Descripción	Esta regla especifica el tiempo que un dispositivo BlackBerry guarda en la memoria caché la dirección del servidor PGP Universal Server.
Ejemplo	BlackBerry recuperan la política de correo electrónico de PGP Universal Server para determinar si los mensajes de correo electrónico se deben firmar, cifrar o firmar y cifrar. Si la política de correo electrónico no cambia con frecuencia, puede establecer esta regla de modo que los dispositivos recuperen la política de correo electrónico de PGP Universal Server cada 48 horas.
Valores posibles	• De 4 a 48 horas
Valor predeterminado	• 24 horas
Requisitos mínimos	• PGP Support Package para smartphones BlackBerry 4.1 • BlackBerry Device Software 4.1
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP2

Regla de política de TI Dirección de PGP Universal Server

Descripción	Esta regla especifica la dirección de PGP Universal Server de su empresa. PGP Universal Server aplica las políticas de correo electrónico que el administrador del servidor PGP Universal Server configura. Configure esta regla para solicitar que el usuario del dispositivo BlackBerry se registre con PGP Universal Server. Al registrarse, un dispositivo BlackBerry con PGP Support Package para smartphones BlackBerry impone la conformidad con las políticas de correo electrónico en todos los mensajes de correo electrónico.
Valor predeterminado	• Valor nulo

Requisitos mínimos	• PGP Support Package para smartphones BlackBerry 4.1 • BlackBerry Device Software 4.1
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP2

Grupo de políticas de aplicaciones de valor añadido de RIM

Regla de política de TI Desactivar el acceso a los datos del organizador para aplicaciones de redes sociales

Descripción	Esta regla especifica si un dispositivo BlackBerry debe impedir que las aplicaciones de redes sociales obtengan acceso a los datos del organizador.
Ejemplo	El personal de soporte técnico de una universidad usa Facebook para smartphones BlackBerry para compartir información sobre cursos, programaciones de tutoría y contactos de ayuda. Puede permitir aplicaciones de redes sociales para acceder a la información del calendario e información de contacto en disponibles para que el personal de soporte técnico pueda compartir la información con los estudiantes que usen la aplicación.
Valores posibles	• Sí • No
Valor predeterminado	• Sí
Requisitos mínimos	• BlackBerry Device Software 4.2.0
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP3

Grupo de políticas de seguridad

Regla de política de TI Permitir conexiones externas

Descripción	Esta regla especifica si las aplicaciones, incluidas aplicaciones de terceros, pueden iniciar conexiones externas (por ejemplo, gateways WAP).
Valores posibles	• Sí • No
Valor predeterminado	• Sí
Requisitos mínimos	• BlackBerry Device Software 3.6
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP2

Regla de política de TI Permitir el restablecimiento del temporizador de inactividad

Descripción	Esta regla especifica si un dispositivo BlackBerry permite a aplicaciones de terceros volver a configurar el valor de tiempo de espera de inactividad en el dispositivo y desviar el valor de tiempo de espera para la contraseña del dispositivo. Si necesita más información acerca del tiempo de espera de inactividad, visite www.blackberry.com/go/apiref para leer la clase EventInjector y el método Backlight.enable() en la referencia de API de BlackBerry Java Development Environment.
Valores posibles	• Sí • No

Valor predeterminado	• No
Requisitos mínimos	• BlackBerry Device Software 4.2.1
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP2

Regla de política de TI Permitir conexiones en ambos sentidos

Descripción	Esta regla especifica si las aplicaciones, incluidas aplicaciones de terceros, pueden abrir conexiones internas y externas simultáneamente en un dispositivo BlackBerry. Una aplicación puede generar un problema de seguridad si abre conexiones internas y externas al mismo tiempo, ya que la aplicación puede recopilar datos del interior del firewall y enviarlos fuera del mismo.
Valores posibles	• Sí • No
Valor predeterminado	• No
Requisitos mínimos	• BlackBerry Device Software 3.6
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP2

Regla de política de TI Permitir que aplicaciones de otros fabricantes usen el puerto serie

Descripción	Esta regla especifica si las aplicaciones de terceros pueden utilizar los puertos serie, IrDA o USB en un dispositivo BlackBerry.
Ejemplo	BlackBerry de su empresa usan una aplicación personalizada que les permite cargar en sus ordenadores los datos de cliente que recopilan durante sus visitas fuera de la oficina. La aplicación

	requiere el uso del puerto USB en los dispositivos activados para conectarse a ordenadores. Puede utilizar esta regla para permitir que la aplicación utilice el puerto USB en los dispositivos.
Valores posibles	• Sí • No
Valor predeterminado	• Sí
Requisitos mínimos	• BlackBerry Device Software 3.6
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP2

Regla de política de TI Intensidad de protección de contenido

Descripción	Esta regla especifica la intensidad del cifrado que utiliza el dispositivo BlackBerry para la protección de contenido de los datos que recibe cuando está bloqueado. Al especificar un valor para esta regla, se activa la protección de contenido. Si configura esta regla en Alta, el dispositivo utiliza una clave pública ECC de 160 bits. Si configura esta regla en Muy alta, el dispositivo utiliza una clave pública ECC de 283 bits. Si configura esta regla en Extremadamente alta, el dispositivo utiliza una clave pública ECC de 571 bits. Para dispositivos que ejecutan BlackBerry Device Software 5.0 y posterior con memoria de dispositivo integrada, esta regla también cifra la memoria de dispositivo integrada con la contraseña del usuario del dispositivo BlackBerry y una clave generada por el dispositivo. Los archivos multimedia en la memoria integrada del dispositivo no se cifran a menos que establezca la regla de política de TI Cifrado en archivos multimedia de la memoria de dispositivo integrada. Para dispositivos que ejecutan BlackBerry Device Software 4.7 y anterior, puede configurar la regla de política de TI Nivel de cifrado del sistema de archivos externo para cifrar los archivos multimedia en la tarjeta de memoria.
Reglas relacionadas	La regla de política de TI Contraseña necesaria afecta a esta regla. Un dispositivo utiliza esta regla sólo si configura la regla de política de TI Contraseña necesaria como Sí. Esta regla afecta a la regla de política de TI Longitud mínima de la contraseña. Si configura esta regla como Muy alta, debe configurar la regla de política de TI Longitud de contraseña mínima como 12 caracteres. Si configura esta regla como Extremadamente alta, debe configurar la regla de política de TI Longitud de contraseña mínima como 21 caracteres.

Valores posibles	• Alta • Más alta • Extremadamente alta
Valores predeterminados	• Valor nulo
Requisitos mínimos	• BlackBerry Device Software 4.0
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de TI Desactivar 3DES Transport Crypto

Descripción	Esta regla especifica si se debe impedir que un dispositivo BlackBerry utilice el algoritmo Triple DES para cifrar y descifrar los datos.
Valores posibles	• Sí • No
Valor predeterminado	• No
Requisitos mínimos	• BlackBerry Device Software 4.0
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP2

Regla de política de TI Desactivar la memoria externa

Descripción	Esta regla especifica si se impide que un usuario de dispositivo BlackBerry acceda a la tarjeta de memoria de un dispositivo BlackBerry.

Valores posibles	• Sí • No
Valor predeterminado	• No
Requisitos mínimos	• BlackBerry Device Software 4.2
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de TI Desactivar GPS

Descripción	Esta regla especifica si está activada la característica GPS de un dispositivo BlackBerry. Si configura esta regla en Sí, BlackBerry Maps no funciona y las aplicaciones no pueden obtener acceso a las API del GPS del dispositivo.
Reglas relacionadas	Esta regla afecta a la configuración de la regla de política de control de aplicaciones "¿Se permite el acceso a la API del GPS?". Esta regla anula la configuración de la regla de política de control de aplicaciones "¿Se permite el acceso a la API del GPS?".
Valores posibles	• Sí • No
Valor predeterminado	• No
Requisitos mínimos	• BlackBerry Device Software 4.3
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP2

Regla de política de TI Desactivar módem IP

Descripción	Esta regla especifica si está disponible el módem IP de un dispositivo BlackBerry.

Valores posibles	• Sí • No
Valor predeterminado	• No
Requisitos mínimos	• BlackBerry Device Software 4.0
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de TI Desactivar el almacenamiento masivo USB

Descripción	Esta regla especifica si el almacenamiento masivo USB y el protocolo de transferencia multimedia están activados. El protocolo de transferencia multimedia permite que un usuario del dispositivo BlackBerry transfiera archivos multimedia desde un ordenador o BlackBerry Desktop Manager a un dispositivo BlackBerry o una tarjeta de memoria. Cuando transfiere archivos mediante el protocolo de transferencia multimedia, el dispositivo no protege los archivos usando la protección de contenido y no codifica los datos en la tarjeta de memoria, incluso si se ha configurado la regla de política de TI Nivel de cifrado del sistema de archivos externo. Esta característica no está disponible en BlackBerry Desktop Manager 4.2.2, ya que Roxio Media Manager utiliza el protocolo de transferencia multimedia para transferir archivos. Para obtener más información sobre la protección de datos que el dispositivo almacena en una tarjeta de memoria, consulte la *Descripción técnica general sobre seguridad de BlackBerry Enterprise Solution* .
Valores posibles	• Sí • No
Valores predeterminados	• Sí en la política de TI Predeterminada.
Requisitos mínimos	• BlackBerry Device Software 4.2

Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP2

Regla de política de TI Desactivar la descarga de aplicaciones de otros fabricantes

Descripción	Esta regla especifica si un usuario del dispositivo BlackBerry puede instalar o actualizar aplicaciones en un dispositivo BlackBerry mediante BlackBerry Browser o BlackBerry App World. Si configura esta regla en Sí, el usuario no puede instalar ni actualizar aplicaciones en el dispositivo mediante BlackBerry Browser o BlackBerry App World. El usuario puede instalar o actualizar una aplicación que crea Research In Motion mediante BlackBerry Desktop Software. Esta regla no se aplica a las aplicaciones de complemento de RIM en las configuraciones de software. Si configura esta regla en Sí, el BlackBerry Administration Service le impide utilizar una configuración de software para instalar aplicaciones de terceros que son firmadas digitalmente por medio de claves de firma de código en el dispositivo. Después de que aplique esta regla, cualquier aplicación de terceros firmada es eliminada del dispositivo y el usuario no puede volver a instalarlas.
Reglas relacionadas	Esta regla afecta a la regla de política de TI Regla de restricción de aplicaciones. Si configura esta regla a Sí, tiene prioridad sobre la regla de política de TI Regla de restricción de aplicaciones. Esta regla afecta a la regla de política de TI Regla de restricción de categorías. Si configura esta regla a Sí, tiene prioridad sobre la regla de política de TI Regla de restricción de categorías. La regla de política de TI Métodos de instalación de aplicaciones afecta a esta regla. Si desactiva los métodos de aplicación específicos mediante la regla Métodos de instalación de aplicaciones, la regla Métodos de instalación de aplicaciones tiene prioridad sobre dispositivos BlackBerry 7.1 y superiores.
Valores posibles	• Sí • No
Valores predeterminados	• No en la política de TI Predeterminada
Requisitos mínimos	• BlackBerry Device Software 3.6
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de TI Cifrado en archivos multimedia de la memoria de dispositivo integrada

Descripción	Esta regla especifica si los archivos multimedia ubicados en la memoria integrada de un dispositivo BlackBerry se cifran en la contraseña de usuario del dispositivo BlackBerry y en la clave generada por el dispositivo.
Reglas relacionadas	La regla de política de TI Intensidad de protección de contenido afecta a esta regla. El dispositivo utiliza esta regla sólo si también ha configurado la regla de política de TI Intensidad de protección de contenido.
Valores posibles	• Permitido • necesaria • No permitido
Valor predeterminado	• Permitido
Requisitos mínimos	• BlackBerry Device Software 5.0
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de TI Nivel de cifrado del sistema de archivos externo

Descripción	Esta regla especifica el nivel de cifrado que utiliza un dispositivo BlackBerry para cifrar los archivos que almacena en una tarjeta de memoria. Puede utilizar esta regla para solicitar que el dispositivo cifre una tarjeta de memoria, incluyendo o excluyendo los archivos de la tarjeta de memoria. No es posible utilizar esta regla para cifrar los archivos que el usuario del dispositivo BlackBerry transfiere a la tarjeta de memoria manualmente (por ejemplo, desde un dispositivo de almacenamiento masivo USB). Las claves principales de la tarjeta de memoria se almacenan en la tarjeta de memoria. Un dispositivo está diseñado para utilizar las claves principales para descifrar y cifrar archivos en la tarjeta de

	memoria. Un dispositivo está diseñado para utilizar su clave, una contraseña indicada por el usuario o ambas para cifrar las claves principales.
Valores posibles	• Cifrar con la contraseña de usuario (excluyendo los directorios multimedia) • Cifrar con la contraseña de usuario (incluyendo los directorios multimedia) • Cifrar con la clave del dispositivo (excluyendo los directorios multimedia) • Cifrar con la clave del dispositivo (incluyendo los directorios multimedia) • Cifrar con la contraseña del usuario y la clave del dispositivo (excluyendo los directorios multimedia) • Cifrar con la contraseña del usuario y la clave del dispositivo (incluyendo los directorios multimedia) • No necesario
Valores predeterminados	• No necesario
Requisitos mínimos	• BlackBerry Device Software 4.2
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de TI Imponer bloqueo si el dispositivo está en la funda

Descripción	Esta regla especifica si un dispositivo BlackBerry se bloquea cuando un usuario de dispositivo BlackBerry lo mete en la funda.
Valores posibles	• Sí • No
Valores predeterminados	• No en la política de TI Predeterminada
Requisitos mínimos	• BlackBerry Device Software 3.6

Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de TI Patrón de la contraseña necesaria

Descripción	Esta regla especifica el patrón necesario para una contraseña del dispositivo BlackBerry. Un carácter en el patrón de la contraseña especifica el tipo de carácter permitido en su posición en la contraseña. Las contraseñas pueden sólo contener caracteres Latín-1. Si configura esta regla, el usuario del dispositivo BlackBerry puede crear una contraseña mayor o igual que la longitud del patrón en un dispositivo. Los caracteres de la contraseña que excedan la longitud del patrón pueden ser cualquier letra, número o símbolo. Puede utilizar los siguientes caracteres para especificar el patrón de la contraseña: • a: Permite cualquier letra. • A: Permite sólo una letra mayúscula. • c: Permite cualquier consonante • C: Permite sólo una consonante mayúscula. • v: Permite cualquier vocal. • V: Permite sólo una vocal mayúscula. • N, n o #: Permite sólo un número. • S, s o @: Permite sólo un símbolo. • ?: Permite cualquier letra, número o símbolo.
Valor predeterminado	• Valor nulo
Requisitos mínimos	• BlackBerry Device Software 4.2
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP2

Regla de política de TI Restablecer valores predeterminados de serie al borrar

Descripción	Esta regla especifica si un dispositivo BlackBerry restablece los valores predeterminados de serie al recibir el comando de administración de TI Eliminar todos los datos del dispositivo y desactivar el dispositivo a través de la red inalámbrica. Para dispositivos que ejecutan BlackBerry Device Software 5.0 y posterior, esta regla se impone tanto de forma remota (cuando un administrador borra los datos en un dispositivo de forma remota) como de forma local (por ejemplo, cuando un usuario del dispositivo BlackBerry excede el máximo número de veces que el usuario puede intentar escribir la contraseña o borra todos los datos del dispositivo). Para dispositivos que se ejecutan BlackBerry Device Software 4.7 y anterior, esta regla se impone sólo cuando un administrador borra los datos de forma remota.
Valores posibles	• Sí • No
Valor predeterminado	• No
Requisitos mínimos	• BlackBerry Device Software 4.2.2
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP2

Regla de política de TI Algoritmos hash del archivo Cod del transcodificador de seguridad

Descripción	Esta regla especifica los algoritmos hash de los archivos .cod del transcodificador que utiliza el dispositivo BlackBerry para registrar el transcodificador. Configure cada uno de los algoritmos hash en formato hexadecimal y separe los distintos valores con una coma (,).
Valor predeterminado	• Valor nulo

Requisitos mínimos	• BlackBerry Device Software 4.5
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP3

Grupo de políticas de aplicación S/MIME

Las reglas de política de TI del grupo de políticas de aplicación S/MIME se aplican a dispositivos BlackBerry que ejecutan S/MIME Support Package para smartphones BlackBerry. Para obtener más información sobre el uso de S/MIME Support Package para smartphones BlackBerry, consulte *Información general técnica de seguridad de S/MIME Support Package para dispositivos BlackBerry* .

Regla de política de TI Dirección de correo electrónico del servidor de mensajería de confianza (EMS)

Descripción	Esta regla especifica la dirección de correo electrónico para el Entrust Entelligence Messaging Server de la empresa.
Ejemplo	Su empresa utiliza Entrust Entelligence Messaging Server para proteger los mensajes correo electrónico que envían los empleados. Puede utilizar esta regla para permitir que los dispositivos BlackBerry se comuniquen con EMS y admitan la funcionalidad EMPLEADOS que se integra con los dispositivos.
Valor predeterminado	• Valor nulo
Requisitos mínimos	• BlackBerry Device Software 4.0 • S/MIME Support Package para smartphones BlackBerry 4.0
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP2

Regla de política de TI Cifrados de contenido S/MIME permitido

Descripción	Esta regla especifica los algoritmos de cifrado que un dispositivo BlackBerry puede utilizar para cifrar mensajes de correo electrónico protegidos S/MIME. Para mantener la compatibilidad con la mayoría de los clientes S/MIME, utilice el cifrado Triple DES y uno de los algoritmos RC2. De forma predeterminada, el dispositivo está diseñado para cifrar los mensajes de correo electrónico mediante cifrado Triple DES cuando no conoce la capacidad de descifrado de un destinatario.
Ejemplo	Instala S/MIME Support Package para smartphones BlackBerry en los dispositivos para permitir a los usuarios que envíen y reciban correo electrónico firmado con S/MIME y firmados y cifrados con S/MIME, así como mensajes PIN. Su empresa únicamente admite el uso de AES y Triple DES, por lo que usa esta regla para permitir que los dispositivos usen estos cifrados de contenido para cifrar los mensajes S/MIME.
Valores posibles	• AES (256 bits) • AES (192 bits) • AES (128 bits) • CAST (128 bits) • RC2 (128 bits) • Triple DES • RC2 (64 bits) • RC2 (40 bits)
Valor predeterminado	• AES (256 bits), AES (192 bits), AES (128 bits), CAST (128 bits), RC2 (128 bits) y Triple DES
Requisitos mínimos	• BlackBerry Device Software 3.6 • S/MIME Support Package para smartphones BlackBerry 1.5
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de TI S/MIME Allowed Encrypted Attachment Mode

Descripción	Esta regla especifica el modo de recuperar información de archivos adjuntos protegidos S/MIME en un dispositivo BlackBerry.
Ejemplo	Los estándares de seguridad de su empresa especifican que los usuarios de dispositivos BlackBerry sólo deben abrir los archivos adjuntos de mensajes cifrados con S/MIME en sus ordenadores en un entorno de trabajo de alta seguridad únicamente. Puede utilizar esta regla para evitar que los usuarios recuperen los archivos adjuntos cifrados con S/MIME en sus dispositivos.
Valores posibles	• Automático • Manual • Ninguno
Valor predeterminado	• Automático
Requisitos mínimos	• BlackBerry Device Software 4.5
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP2

Regla de política de TI Tipos de cifrado S/MIME permitidos

Descripción	Esta regla especifica los tipos de cifrado que un dispositivo BlackBerry puede utilizar con mensajería de correo electrónico protegida S/MIME.
Ejemplo	Algunos usuarios de su empresa tienen previsto un proyecto confidencial y quieren mantener la seguridad de sus mensajes de correo electrónico. Instala S/MIME Support Package para smartphones BlackBerry en los dispositivos para permitir a los usuarios de dispositivos BlackBerry que envíen y reciban correo electrónico firmado con S/MIME y firmados y cifrados con S/MIME, así como mensajes PIN. Puede configurar esta regla de política de TI para que los usuarios deban utilizar una contraseña compartida para cifrar y descifrar los mensajes de correo electrónico.

Valores posibles	• Cifrado basado en certificado • Cifrado basado en contraseña • Ambas
Valor predeterminado	• Ambas
Requisitos mínimos	• BlackBerry Device Software 4.6 • S/MIME Support Package para smartphones BlackBerry 4.0
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP2

Regla de política de TI S/MIME fuerza la firma digital

Descripción	Esta regla especifica si el dispositivo BlackBerry envía todos los mensajes de correo electrónico protegidos S/MIME con una firma digital.
Ejemplo	Instala S/MIME Support Package para smartphones BlackBerry en los dispositivos para permitir a los usuarios que envíen y reciban mensajes PIN y mensajes de correo electrónico firmados con S/MIME y firmados y cifrados con S/MIME. Los estándares de seguridad de su empresa requieren que todos los mensajes de correo electrónico se deben firmar digitalmente. Las firmas digitales se usan para verificar que un correo electrónico lo ha enviado el usuario correcto. Puede utilizar esta regla para agregar firmas digitales a todos los mensajes S/MIME que los usuarios envían desde los dispositivos.
Valores posibles	• Sí • No
Valor predeterminado	• No
Requisitos mínimos	• BlackBerry Device Software 3.6 • S/MIME Support Package para smartphones BlackBerry 1.5
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP2

Regla de política de TI S/MIME fuerza los mensajes cifrados

Descripción	Esta regla especifica si un dispositivo BlackBerry debe cifrar todos los mensajes de correo electrónico que un usuario del dispositivo BlackBerry envía mediante el cifrado S/MIME.
Ejemplo	Debe instalar S/MIME Support Package para smartphones BlackBerry en los dispositivos para permitir a los usuarios que envíen y reciban mensajes de correo electrónico firmado con S/MIME y firmados y cifrados con S/MIME, así como mensajes PIN. Para cumplir los requisitos de su empresa a fin de obtener una comunicación móvil de alta seguridad, puede usar esta regla para que los dispositivos cifren todos los mensajes de correo electrónico que los usuarios reenvían o a los que responden mediante el cifrado S/MIME.
Valores posibles	• Sí • No
Valor predeterminado	• No
Requisitos mínimos	• BlackBerry Device Software 3.6 • S/MIME Support Package para smartphones BlackBerry 1.5
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de TI Longitud mínima de la clave ECC fuerte S/MIME

Descripción	Esta regla especifica el tamaño de clave Diffie-Hellman mínimo que se debe utilizar con los mensajes de correo electrónico protegidos S/MIME.
Ejemplo	Los dispositivos BlackBerry usan claves públicas S/MIME y claves privadas S/MIME para cifrar y descifrar mensajes de correo electrónico. Las claves S/MIME pueden usar el algoritmo DH para el cifrado y descifrado. La longitud de la clave en bits es un factor para determinar la intensidad de la clave. Su empresa admite una longitud de clave mínima de 512 bits para las claves que usan el

	algoritmo DH, por lo que especifica 512 bits en esta regla para permitir que los dispositivos admitan claves S/MIME de esta longitud o superior.
Valores posibles	• De 512 a 4096 bits
Valor predeterminado	• 1024 bits
Requisitos mínimos	• BlackBerry Device Software 3.6 • S/MIME Support Package para smartphones BlackBerry 1.5
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP2

Regla de política de TI Longitud mínima de la clave DSA fuerte S/MIME

Descripción	Esta regla especifica el tamaño mínimo de la clave DSA que un dispositivo BlackBerry utiliza con mensajes de correo electrónico protegidos S/MIME.
Ejemplo	Los dispositivos BlackBerry usan claves públicas S/MIME y claves privadas S/MIME para cifrar y descifrar mensajes de correo electrónico. Las claves S/MIME pueden usar el algoritmo DSA para el cifrado y descifrado. La longitud de la clave en bits es un factor para determinar la intensidad de la clave. Su empresa admite una longitud de clave mínima de 512 bits para las claves que usan el algoritmo DSA, por lo que especifica 512 bits en esta regla para permitir que los dispositivos admitan claves S/MIME de esta longitud o superior.
Valores posibles	• De 512 a 1024 bits
Valor predeterminado	• 1024 bits
Requisitos mínimos	• BlackBerry Device Software 3.6 • S/MIME Support Package para smartphones BlackBerry 1.5
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP2

Regla de política de TI Longitud mínima de la clave ECC fuerte S/MIME

Descripción	Esta regla especifica el tamaño mínimo de la clave ECC que un dispositivo BlackBerry utiliza con mensajes de correo electrónico protegidos S/MIME.
Ejemplo	Los dispositivos BlackBerry usan claves públicas S/MIME y claves privadas S/MIME para cifrar y descifrar mensajes de correo electrónico. Las claves S/MIME pueden usar el algoritmo ECC para el cifrado y descifrado. La longitud de la clave en bits es un factor para determinar la intensidad de la clave. Su empresa admite una longitud de clave mínima de 160 bits para las claves que usan el algoritmo ECC, por lo que especifica 160 bits en esta regla para permitir que los dispositivos admitan claves S/MIME de esta longitud o superior.
Valores posibles	• De 163 a 571 bits
Valor predeterminado	• 163 bits
Requisitos mínimos	• BlackBerry Device Software 3.6 • S/MIME Support Package para smartphones BlackBerry 1.5
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP2

Regla de política de TI Longitud mínima de la clave RSA fuerte S/MIME

Descripción	Esta regla especifica el tamaño mínimo de la clave RSA que un dispositivo BlackBerry utiliza con mensajes de correo electrónico protegidos S/MIME.
Ejemplo	Los dispositivos BlackBerry usan claves públicas S/MIME y claves privadas S/MIME para cifrar y descifrar mensajes de correo electrónico. Las claves S/MIME pueden usar el algoritmo RSA para el cifrado y descifrado. La longitud de la clave en bits es un factor para determinar la intensidad de la clave. Su empresa admite una longitud de clave mínima de 512 bits para las claves que usan el algoritmo RSA, por lo que especifica 512 bits en esta regla para permitir que los dispositivos admitan claves S/MIME de esta longitud o superior.

Valores posibles	• De 512 a 4096 bits
Valor predeterminado	• 1024 bits
Requisitos mínimos	• BlackBerry Device Software 3.6 • S/MIME Support Package para smartphones BlackBerry 1.5
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP2

Regla de política de TI Modo mensaje completo y envío S/MIME

Descripción	Esta regla especifica el modo en que el dispositivo BlackBerry recupera el texto completo de un mensaje de correo electrónico cuando un usuario del dispositivo BlackBerry responde o reenvía el mensaje de correo electrónico.
Ejemplo	De forma predeterminada, los usuarios de dispositivos BlackBerry deben solicitar el texto completo de los mensajes de correo electrónico a los que responden o reenvían como mensajes S/MIME desde sus dispositivos. Puede utilizar esta regla para que los dispositivos recuperen y muestren automáticamente el texto completo de los mensajes de correo electrónico a los que responden los usuarios o reenvían como mensajes S/MIME.
Valores posibles	• Automático • Manual • Ninguno
Valor predeterminado	• Manual
Requisitos mínimos	• BlackBerry Device Software 5.0
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP2

Grupo de políticas de la VPN

Regla de política de TI Nombre de usuario de VPN

Descripción	Esta regla especifica el nombre de usuario predeterminado que un dispositivo BlackBerry utiliza para iniciar sesión en el servidor VPN de su empresa. Especifique un valor para esta regla si desea configurar un nombre de usuario predeterminado para todas las cuentas de usuario. Si un usuario de dispositivo BlackBerry introduce un nombre de usuario en un dispositivo manualmente, las actualizaciones de política de TI sobrescriben o eliminan el valor introducido por el usuario. Para conservar el valor del dispositivo, compruebe que en la regla actualizada se utiliza el mismo valor que en esta regla.
Valor predeterminado	• Valor nulo
Requisitos mínimos	• BlackBerry Device Software 4.0
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de TI Contraseña de usuario de VPN

Descripción	Esta regla especifica la contraseña predeterminada que utiliza un dispositivo BlackBerry para iniciar sesión en el servidor VPN de su empresa. Especifique un valor para esta regla si desea configurar una contraseña predeterminada para todas las cuentas de usuario. Si un usuario de dispositivo BlackBerry introduce una contraseña en un dispositivo manualmente, las actualizaciones de política de TI sobrescriben o eliminan el valor introducido por el usuario. Para conservar el valor del dispositivo, compruebe que en la regla actualizada se utiliza el mismo valor que en esta regla.
Valor predeterminado	• Valor nulo
Requisitos mínimos	• BlackBerry Device Software 4.0

Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Grupo de políticas de Wi-Fi

El nombre anterior de este grupo de políticas era Grupo de políticas de WLAN.

Regla de política de TI Desactivar Wi-Fi

Descripción	Esta regla especifica si un usuario de dispositivo BlackBerry puede acceder a una red Wi-Fi desde un dispositivo BlackBerry habilitado para Wi-Fi.
Valores posibles	• Sí • No
Valor predeterminado	• No
Requisitos mínimos	• BlackBerry Device Software 4.2.1
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Grupo de políticas Actualizaciones de software con cable

Las reglas de política de TI del grupo de políticas Actualizaciones de software con cable se aplican al proceso de actualización de BlackBerry Device Software cuando un usuario del dispositivo BlackBerry conecta un dispositivo BlackBerry a un ordenador.

Regla de política de TI Permitir la carga de software basado en Web

Descripción	Esta regla especifica si un usuario de dispositivo BlackBerry puede actualizar BlackBerry Device Software a través de la característica de carga de software a través de Internet.
Ejemplo	Su empresa tiene poco personal de TI. Desea que los empleados puedan actualizar BlackBerry Device Software en sus dispositivos sin tener que solicitar una actualización al departamento de TI. Puede utilizar esta regla para permitir a los usuarios actualizar BlackBerry Device Software mediante el sitio Web de BlackBerry Device Software (www.blackberry.com/update).
Valores posibles	• Sí • No
Valor predeterminado	• No
Requisitos mínimos	• BlackBerry Device Software 5.0
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de TI Copia de seguridad de servicios criptográficos

Descripción	Esta regla especifica si el dispositivo BlackBerry puede realizar copias de seguridad de los datos de servicios criptográficos cuando el usuario del dispositivo BlackBerry actualiza BlackBerry Device Software. Un servicio de cifrado es cualquier servicio que utiliza una clave de cifrado para proteger la comunicación en el dispositivo. Si permite al dispositivo realizar copias de seguridad de los datos de los servicios criptográficos, el dispositivo puede seguir utilizando los servicios criptográficos una vez se completa el proceso de carga de software sin requerir al usuario que reactive el dispositivo manualmente.
Valores posibles	• Sí • No

Valor predeterminado	• Sí
Requisitos mínimos	• BlackBerry Device Software 5.0
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Grupo de políticas de actualizaciones inalámbricas de software

Regla de política de TI Desactivar la descarga de revisiones a través de WAN en itinerancia

Descripción	Esta regla especifica si se impide que un dispositivo BlackBerry descargue actualizaciones de BlackBerry Device Software a través de una conexión WAN cuando se encuentre en itinerancia.
Ejemplo	No desea que los usuarios de dispositivos BlackBerry actualicen BlackBerry Device Software a través de la red inalámbrica mediante una conexión WAN en itinerancia, debido a que este tipo de conexión no cumple los requisitos de seguridad y los estándares de uso de red de su empresa. Puede utilizar esta regla para evitar que los usuarios actualicen BlackBerry Device Software mediante una conexión WAN en itinerancia.
Valores posibles	• Sí • No
Valor predeterminado	• No
Requisitos mínimos	• BlackBerry Device Software 4.5
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Ajustes de configuración

5

Opciones de configuración de perfiles Wi-Fi

Configuración de la autoridad de certificación asociada

Descripción	Esta configuración especifica el nombre de perfil de la autoridad de certificación que se ha configurado en la regla de política de TI Nombre del perfil de la autoridad de certificación. El perfil de la autoridad de certificación consta de credenciales que un dispositivo BlackBerry puede utilizar para iniciar un proceso de inscripción de certificado. Después de asociar un perfil de autoridad de certificación a un perfil Wi-Fi, puede asignar el perfil Wi-Fi a una cuenta de usuario y enviarlo al dispositivo.
Valor predeterminado	• Valor nulo
Requisitos mínimos	• BlackBerry Device Software 5.0

Opción Perfil VPN asociado

Descripción	Esta configuración especifica el nombre del perfil VPN que desea asociar al perfil Wi-Fi.
Valor predeterminado	• Valor nulo
Requisitos mínimos	• BlackBerry Device Software 4.2.0

Opción de configuración Permitir la comunicación entre puntos de acceso Wi-Fi

Descripción	Esta configuración especifica si un dispositivo BlackBerry puede establecer comunicaciones Wi-Fi entre puntos de acceso inalámbricos.
Valores posibles	• Sí • No
Valor predeterminado	• Sí
Requisitos mínimos	• BlackBerry Device Software 4.2.1

Opción de configuración Permitir cambios de Wi-Fi en el dispositivo

Descripción	Esta configuración especifica si un usuario del dispositivo BlackBerry puede cambiar la configuración de políticas de Wi-Fi en un dispositivo BlackBerry.
Valores posibles	• Sí • No
Valor predeterminado	• Sí
Requisitos mínimos	• BlackBerry Device Software 4.0

Opción de configuración Permitir guardar contraseña de Wi-Fi

Descripción	Esta configuración especifica si un usuario de dispositivo BlackBerry puede guardar las contraseñas de autenticación en una red Wi-Fi en un dispositivo BlackBerry.
Valores posibles	• Sí • No
Valor predeterminado	• Sí
Requisitos mínimos	• BlackBerry Device Software 4.2.1

Opción de configuración Tipo de banda Wi-Fi

Descripción	Esta configuración especifica los tipos de banda en los que se configura que pueden operar los puntos de acceso inalámbrico de un determinado SSID.
Valores posibles	• 802.11 a/b/g • 802.11 b/g • 802.11 a • 802.11 b
Valor predeterminado	• 802.11 a/b/g
Requisitos mínimos	• BlackBerry Device Software 4.2.2

Opción de configuración Modo de acceso Wi-Fi de BlackBerry Infrastructure Wi-Fi

Descripción	Esta configuración especifica si un dispositivo BlackBerry se puede conectar a BlackBerry Infrastructure a través de una red Wi-Fi.
Configuración relacionada	Esta opción de configuración afecta a la regla de política de TI Modo de acceso Wi-Fi de BlackBerry Infrastructure. Si cambia esta configuración, se anula la regla de política de TI BlackBerry Infrastructure con modo de acceso Wi-Fi. Puede utilizar esta configuración para configurar el modo de acceso para una red Wi-Fi específica y la regla de política de TI para configurar el modo de acceso para otras redes Wi-Fi. La regla de política de TI Modo de acceso Wi-Fi de BlackBerry Infrastructure afecta a esta opción de configuración. Si desactiva el acceso a BlackBerry Infrastructure a través de una red Wi-Fi utilizando la regla de política de TI Modo de acceso Wi-Fi de BlackBerry Infrastructure, no puede anular la regla de política de TI utilizando esta configuración.
Valores posibles	• El acceso no requiere VPN • El acceso requiere VPN • Acceso deshabilitado
Valor predeterminado	• El acceso no requiere VPN
Requisitos mínimos	• BlackBerry Device Software 5.0

Opción de configuración Gateway predeterminada de Wi-Fi

Descripción	Esta regla especifica la gateway predeterminada en el formato de dirección IP (por ejemplo, 10.0.0.1) que un dispositivo BlackBerry puede utilizar si DHCP está desactivado en el dispositivo.
Configuración relacionada	La opción Configuración del DHCP en Wi-Fi afecta a esta opción de configuración. Un dispositivo utiliza esta configuración sólo si se cambia la opción de configuración Configuración del DHCP en Wi--Fi a No.

Valor predeterminado	• Valor nulo
Requisitos mínimos	• BlackBerry Device Software 4.2

Ajuste de configuración ID de clave predeterminada de Wi-Fi

Descripción	Esta configuración especifica el ID de clave WEP predeterminado. Compruebe que el ID de clave WEP coincide con el ID del punto de acceso WEP y la clave WEP correspondiente.
Valores posibles	• De 1 a 4
Valor predeterminado	• 1
Requisitos mínimos	• BlackBerry Device Software 4.0

Opción de configuración Configuración del DHCP en Wi-Fi

Descripción	Esta configuración especifica si su empresa utiliza DHCP para la configuración de red dinámica. Si su empresa utiliza una red Wi-Fi que incluye subredes, active DHCP para permitir la itinerancia entre subredes.
Valores posibles	• Sí • No
Valor predeterminado	• Sí
Requisitos mínimos	• BlackBerry Device Software 4.2

Opción de configuración Desactivar validación de certificado de servidor para Wi-Fi

Descripción	Esta configuración especifica si un dispositivo BlackBerry requiere un certificado de autoridad del certificado para autenticación en el servidor cuando utiliza un método de autenticación PEAP, EAP--TLS o EAP-TTLS para conectarse a una red Wi-Fi. Si cambia esta configuración a Sí, no se requiere un certificado raíz para el método de autenticación PEAP, EAP-TLS o EAP-TTLS.
Valores posibles	• Sí • No
Valor predeterminado	• No
Requisitos mínimos	• BlackBerry Device Software 5.0

Opción de configuración Sufijo de dominio de Wi-Fi

Descripción	Esta configuración especifica el sufijo para el nombre de dominio interno, en formato FQDN.
Configuración relacionada	La opción Configuración del DHCP en Wi-Fi afecta a esta opción de configuración. Configure esta opción sólo si cambia la opción de configuración Configuración del DHCP en Wi-Fi a No para que DHCP no esté disponible.
Valor predeterminado	• Valor nulo
Requisitos mínimos	• BlackBerry Device Software 4.2.1

Opción de configuración Método de abastecimiento mediante EAP-FAST a través de Wi-Fi

Descripción	Esta configuración especifica el tipo de método de abastecimiento que un dispositivo BlackBerry puede utilizar al autenticarse con una red Wi-Fi mediante autenticación EAP-FAST con PAC. Si desea que el servidor autentique un dispositivo mediante el nombre de usuario y contraseña de la cuenta de usuario y un certificado raíz la primera vez que el dispositivo se conecte, puede seleccionar la opción Autenticado. El dispositivo no se conecta con el servidor si éste no le proporciona un certificado raíz. Si desea que el servidor autentique un dispositivo con el nombre de usuario y la contraseña de la cuenta de usuario sin la autenticación del servidor, puede seleccionar la opción Anónimo. Si desea que el servidor autentique un dispositivo mediante el nombre de usuario y contraseña de la cuenta de usuario, y desea que la configuración del servidor determine si debe tener lugar la autenticación del servidor, puede seleccionar la opción Ambos. Si el servidor presenta un certificado raíz, el dispositivo verifica el servidor mediante el certificado raíz seleccionado. Si el servidor no presenta un certificado raíz, el dispositivo no realiza autenticación del servidor.
Valores posibles	• Anónimo • Autenticado • Ambas
Valor predeterminado	• Anónimo
Requisitos mínimos	• BlackBerry Device Software 5.0

Opción de configuración Activar página de autenticación de Wi-Fi

Descripción	Esta configuración especifica si el navegador de inicio de sesión de Wi-Fi está disponible en un dispositivo BlackBerry. Cambie esta configuración a Sí para permitir que el usuario de un dispositivo BlackBerry inicie sesión en un portal cautivo mediante el dispositivo.

Valores posibles	• Sí • No
Valor predeterminado	• No
Requisitos mínimos	• BlackBerry Device Software 4.0

Opción de configuración Identificador físico de Wi-Fi solicitado

Descripción	Esta configuración especifica si un dispositivo BlackBerry requiere un identificador físico para la autenticación. Cambie esta configuración a Sí si el dispositivo requiere un identificador físico (por ejemplo, RSA SecurID) como parte de la contraseña para la autenticación.
Valores posibles	• Sí • No
Valor predeterminado	• No
Requisitos mínimos	• BlackBerry Device Software 4.2.1

Opción de configuración Modo de autenticación interna de Wi-Fi

Descripción	Esta configuración especifica el modo de autenticación que utiliza un dispositivo BlackBerry para la seguridad EAP tunelada.
Valores posibles	• Ninguno • EAP-MSCHAPV2 • EAP-GTC

	• PAP • CHAP • MSCHAP • MSCHAPV2 • EAP-MD5
Valor predeterminado	• Ninguno
Requisitos mínimos	• BlackBerry Device Software 4.2.1

Ajuste de configuración de Ruta de acceso Wi-Fi a Internet

Descripción	Este ajuste especifica cómo debe acceder a Internet un dispositivo BlackBerry para buscar los perfiles Wi-Fi que configure para su empresa.
Valores posibles	• Acceder mediante Wi-Fi • Acceder mediante BlackBerry MDS Connection Service • Seleccionar automáticamente
Valor predeterminado	• Seleccionar automáticamente
Requisitos mínimos	• BlackBerry 6

Opción de configuración Dirección IP de Wi-Fi

Descripción	Esta configuración especifica la dirección IP (por ejemplo, 10.0.0.1) que un dispositivo BlackBerry puede utilizar si DHCP está desactivado en el dispositivo.
Configuración relacionada	La opción Configuración del DHCP en Wi-Fi afecta a esta opción de configuración. Un dispositivo utiliza esta configuración sólo si se cambia la opción Configuración del DHCP en Wi-Fi a No.

Valor predeterminado	• Valor nulo
Requisitos mínimos	• BlackBerry Device Software 4.2

Opción de configuración Seguridad de Vínculo Wi-Fi

Descripción	Esta configuración especifica el método de autenticación que requiere el dispositivo BlackBerry para acceder a la red Wi-Fi.
Valores posibles	• Seguridad Wi-Fi abierta • WEP • PSK • EAP-PEAP • EAP-LEAP • ESP-TLS • EAP-FAST • EAP-TTLS • EAP-SIM • EAP-AKA
Valor predeterminado	• Seguridad Wi-Fi abierta
Requisitos mínimos	• BlackBerry Device Software 4.0

Opción de configuración Nivel de seguridad mínimo de la clave de cifrado del certificado EAP-TLS de Wi-Fi

Descripción	Esta configuración especifica el nivel de seguridad mínimo para una clave privada que el método de autenticación EAP utiliza con un certificado de cliente.

	Si se cambia esta configuración a Seguridad media, el dispositivo BlackBerry solicita al usuario del dispositivo BlackBerry una sola vez la contraseña del almacén de claves de manera que el dispositivo pueda recuperar la clave privada y cifrar los mensajes de correo electrónico. Una vez que recupera la clave privada, el dispositivo sólo vuelve a recuperarla cuando el usuario lo reinicia. El dispositivo guarda la clave privada en la memoria caché pero no la guarda con el perfil Wi-Fi. Si se cambia esta configuración a Seguridad alta, el dispositivo siempre solicita al usuario la contraseña del almacén de claves cada vez que accede a la clave privada y cifra los mensajes de correo electrónico. El dispositivo no guarda la clave privada sin cifrar con el perfil Wi-Fi. Si se cambia esta configuración a Seguridad baja, el dispositivo solicita al usuario sólo una sola vez la contraseña del almacén de claves de manera que el dispositivo pueda recuperar la clave privada y cifrar los mensajes de correo electrónico. El dispositivo guarda la clave privada sin cifrar con el perfil Wi-Fi.
Valores posibles	• Seguridad baja • Seguridad alta • Seguridad media
Valor predeterminado	• Seguridad baja
Requisitos mínimos	• BlackBerry Device Software 4.0

Opción de configuración Clave Wi-Fi compartida previamente

Descripción	Esta configuración especifica el PSK si utiliza PSK en su empresa para autenticarse en redes Wi-Fi.
Configuración relacionada	La opción de configuración Seguridad de vínculo Wi-Fi afecta a esta opción de configuración. Un dispositivo BlackBerry utiliza esta configuración sólo si configura la opción de configuración Seguridad de vínculo Wi-Fi en PSK.
Valor predeterminado	• Valor nulo
Requisitos mínimos	• BlackBerry Device Software 4.0

Opción de configuración DNS principal de Wi-Fi

Descripción	Esta configuración especifica el DNS principal en formato de dirección IP (por ejemplo, 10.0.0.1) que un dispositivo BlackBerry puede utilizar si está desactivado DHCP en el dispositivo.
Configuración relacionada	La opción Configuración del DHCP en Wi-Fi afecta a esta opción de configuración. Un dispositivo utiliza esta configuración sólo si se cambia la opción de configuración Configuración del DHCP en Wi--Fi a No.
Valor predeterminado	• Valor nulo
Requisitos mínimos	• BlackBerry Device Software 4.2

Opción de configuración Editabilidad del perfil Wi-Fi

Descripción	Esta configuración especifica si un usuario de dispositivo BlackBerry puede cambiar los parámetros del perfil Wi-Fi en un dispositivo BlackBerry. Si cambia esta configuración a Sin editabilidad, el usuario no puede cambiar ningún parámetro del perfil Wi-Fi. Si cambia esta configuración a Editabilidad de las credenciales, el usuario sólo puede cambiar las credenciales de usuario del perfil Wi-Fi.
Valores posibles	• Editabilidad completa • Sin editabilidad • Editabilidad de las credenciales
Valor predeterminado	• Editabilidad completa
Requisitos mínimos	• BlackBerry Device Software 4.2.1

Opción de configuración Visibilidad de perfil Wi-Fi

Descripción	Esta configuración especifica si un usuario de dispositivo BlackBerry puede ver la configuración del perfil Wi-Fi. Si configura este ajuste como Visibilidad limitada, el dispositivo BlackBerry muestra sólo el nombre del perfil. Si configura esta opción como Visibilidad de las credenciales, el dispositivo muestra sólo el nombre del perfil y la información de inicio de sesión del usuario.
Valores posibles	• Visibilidad completa • Visibilidad limitada • Visibilidad de las credenciales
Valor predeterminado	• Visibilidad completa
Requisitos mínimos	• BlackBerry Device Software 4.2.1

Opción de configuración Umbral de roaming de Wi-Fi

Descripción	Esta configuración determina con qué frecuencia el transmisor Wi-Fi del dispositivo BlackBerry busca puntos de acceso inalámbrico cercanos y se conecta en roaming a otro punto de acceso si la calidad de la señal es mejor que la del actual. Si configura este ajuste como Bajo, el dispositivo sólo cambia cuando la calidad de la señal es muy baja. Si configura esta opción en Medio, el dispositivo estará en roaming cuando la calidad de la señal sea de media a baja. Si configura esta opción como Alto, el dispositivo cambiará directamente a los puntos de acceso con una mejor intensidad de señal. Si configura este ajuste en Auto, el dispositivo selecciona los umbrales de roaming automáticamente.
Valores posibles	• Automático • Bajo • Media • Alto
Valor predeterminado	• Automático

Requisitos mínimos	• BlackBerry Device Software 4.2.1

Opción de configuración DNS secundario de Wi-Fi

Descripción	Esta configuración especifica el DNS secundario en formato de dirección IP (por ejemplo, 10.0.0.1) que un dispositivo BlackBerry puede utilizar si está desactivado DHCP en el dispositivo.
Configuración relacionada	La opción Configuración del DHCP en Wi-Fi afecta a esta regla. Un dispositivo utiliza esta configuración sólo si se cambia la opción Configuración del DHCP en Wi-Fi a No.
Valor predeterminado	• Valor nulo
Requisitos mínimos	• BlackBerry Device Software 4.2

Opción de configuración SAN del servidor de Wi-Fi

Descripción	Esta configuración especifica un campo SAN para el certificado del servidor. Si no especifica un campo SAN para el certificado del servidor, el dispositivo BlackBerry acepta cualquier certificado de servidor válido.
Valor predeterminado	• Valor nulo
Requisitos mínimos	• BlackBerry Device Software 4.2.1

Opción de configuración de Asunto del servidor de Wi--Fi

Descripción	Esta configuración especifica el campo Asunto del certificado de servidor. Si no especifica el campo Asunto del certificado de servidor, el dispositivo BlackBerry acepta cualquier certificado de servidor válido.

Valor predeterminado	• Valor nulo
Requisitos mínimos	• BlackBerry Device Software 4.2.1

Opción de configuración SSID de Wi-Fi

Descripción	Esta configuración especifica el nombre de una red Wi-Fi y sus puntos de acceso inalámbrico. El SSID distingue entre mayúsculas y minúsculas y está limitado a 32 caracteres.
Valor predeterminado	• Valor nulo
Requisitos mínimos	• BlackBerry Device Software 4.0

Opción Máscara de subred de Wi-Fi

Descripción	Esta configuración especifica la máscara de subred en formato de dirección IP (por ejemplo, 10.0.0.1) que un dispositivo BlackBerry puede utilizar si está desactivado DHCP en el dispositivo.
Configuración relacionada	La opción Configuración del DHCP en Wi-Fi afecta a esta regla. Un dispositivo utiliza esta configuración sólo si se cambia la opción Configuración del DHCP en Wi-Fi a No.
Valor predeterminado	• Valor nulo
Requisitos mínimos	• BlackBerry Device Software 4.2

Opción de configuración Número de serie del identificador de Wi-Fi

Descripción	Si un dispositivo BlackBerry requiere que se incluya como parte de la contraseña de autenticación un identificador de software, esta configuración especifica el número de serie del identificador de software que se ofrece al dispositivo.

Valor predeterminado	• Valor nulo
Requisitos mínimos	• BlackBerry Device Software 4.2.1

Opción de configuración Nombre de usuario de Wi-Fi

Descripción	Esta configuración especifica el nombre de usuario para la autenticación PEAP o LEAP en un dispositivo BlackBerry. Configure esta opción si desea crear un valor predeterminado para todos los usuarios de dispositivos BlackBerry. Si un usuario escribe manualmente un nombre de usuario en el dispositivo, las actualizaciones de políticas de TI sobrescriben o eliminan el valor introducido por el usuario. Para mantener el valor especificado por el usuario en el dispositivo, compruebe que el perfil Wi-Fi actualizado utilice el mismo valor que el perfil Wi-Fi del dispositivo.
Valor predeterminado	• Valor nulo
Requisitos mínimos	• BlackBerry Device Software 4.0

Opción de configuración Contraseña de usuario de Wi--Fi

Descripción	Esta configuración especifica la contraseña de autenticación PEAP o LEAP en un dispositivo BlackBerry. Configure esta opción si desea crear un valor predeterminado para todos los usuarios de dispositivos BlackBerry. Si el usuario introduce una contraseña en un dispositivo manualmente, las actualizaciones de políticas de TI sobrescriben o eliminan el valor introducido por el usuario. Para mantener el valor especificado por el usuario en el dispositivo, compruebe que el perfil Wi-Fi actualizado utilice el mismo valor que el perfil Wi-Fi del dispositivo.
Valor predeterminado	• Valor nulo
Requisitos mínimos	• BlackBerry Device Software 4.2

Opción de configuración Clave 1 WEP de Wi-Fi

Descripción	Esta configuración especifica la contraseña de la clave 1 WEP usando el formato *xx:xx:xx:xx:xx*. Esta opción de configuración es compatible con los pares 5 ó 13 de dígitos hexadecimales (del 0 al 9 y de la A a la F) que deberá separar con dos puntos (:). Por ejemplo, AB:CD:EF:01:23 o AB:CD:EF:01:23:45:67:89:AB:CD:EF:01:23.
Valor predeterminado	• Valor nulo
Requisitos mínimos	• BlackBerry Device Software 4.0

Opción de configuración Clave 2 WEP de Wi-Fi

Descripción	Esta configuración especifica la contraseña de la clave 2 WEP usando el formato *xx:xx:xx:xx:xx*. Esta configuración es compatible con 5 o 13 pares de dígitos hexadecimales (0 a 9 y A a F) que se deben separar con dos puntos (:). Por ejemplo, AB:CD:EF:01:23 o AB:CD:EF:01:23:45:67:89:AB:CD:EF:01:23.
Valor predeterminado	• Valor nulo
Requisitos mínimos	• BlackBerry Device Software 4.0

Opción de configuración Clave 3 WEP de Wi-Fi

Descripción	Esta configuración especifica la contraseña de la clave 3 WEP usando el formato *xx:xx:xx:xx:xx*. Esta opción de configuración es compatible con los pares 5 ó 13 de dígitos hexadecimales (del 0 al 9 y de la A a la F) que deberá separar con dos puntos (:). Por ejemplo, AB:CD:EF:01:23 o AB:CD:EF:01:23:45:67:89:AB:CD:EF:01:23.
Valor predeterminado	• Valor nulo
Requisitos mínimos	• BlackBerry Device Software 4.0

Opción de configuración Clave 4 WEP de Wi-Fi

Descripción	Esta configuración especifica la contraseña de la clave 4 WEP usando el formato *xx:xx:xx:xx:xx*. Esta opción de configuración es compatible con los pares 5 ó 13 de dígitos hexadecimales (del 0 al 9 y de la A a la F) que deberá separar con dos puntos (:). Por ejemplo, AB:CD:EF:01:23 o AB:CD:EF:01:23:45:67:89:AB:CD:EF:01:23.
Valor predeterminado	• Valor nulo
Requisitos mínimos	• BlackBerry Device Software 4.0

Configuración para perfiles de VPN

Configuración de la autoridad de certificación asociada

Descripción	Esta configuración especifica el nombre de perfil de la autoridad de certificación que se ha configurado en la regla de política de TI Nombre del perfil de la autoridad de certificación. El perfil de la autoridad de certificación consta de credenciales que un dispositivo BlackBerry puede utilizar para iniciar un proceso de inscripción de certificado. Después de asociar un perfil de autoridad de certificación a un perfil VPN, puede asignar el perfil VPN a una cuenta de usuario y enviarlo al dispositivo.
Valor predeterminado	• Valor nulo
Requisitos mínimos	• BlackBerry Device Software 5.0 • BlackBerry Enterprise Server Express 5.0 SP4

Configuración Activar VPN

Descripción	Esta configuración especifica si está activado el cliente VPN de un dispositivo BlackBerry. Si cambia esta configuración a Sí, el dispositivo debe usar un servidor VPN para acceder a una red Wi-Fi. Si cambia esta configuración a No, el dispositivo podría no ser capaz de utilizar una red Wi-Fi que exija acceso VPN o podría requerir el uso de una forma de control de acceso alternativa.
Valores posibles	• Sí • No
Valor predeterminado	• No
Requisitos mínimos	• BlackBerry Device Software 4.2

Configuración Modo de división de túnel

Descripción	Esta configuración especifica si un BlackBerry puede utilizar división de túnel para desviar una conexión activa de VPN.
Valores posibles	• Activar en todas las redes • Desactivar en redes de empresa • Desactivar en todas las redes
Valor predeterminado	• Desactivar en todas las redes
Requisitos mínimos	• BlackBerry Device Software 5.0

Configuración Suprimir el título de VPN

Descripción	Esta configuración especifica si el cuadro de diálogo de VPN se muestra en un dispositivo BlackBerry después de que se conecte al servidor VPN.

Valores posibles	• Sí • No
Valor predeterminado	• Sí
Requisitos mínimos	• BlackBerry Device Software 4.2.1

Configuración Uso de los certificados Xauth de la VPN

Descripción	Esta configuración especifica si el cliente VPN en un dispositivo BlackBerry debe utilizar certificados Xauth para autenticarse en la gateway de VPN de su empresa.
Configuración relacionada	El ajuste de configuración Activar VPN influye en esta configuración. Para que un dispositivo pueda utilizar esta configuración, debe cambiar el valor del parámetro Activar VPN a Sí.
Valores posibles	• Sí • No
Valor predeterminado	• No
Requisitos mínimos	• BlackBerry Device Software 4.2

Configuración Permitir cambios de VPN en el dispositivo

Descripción	Esta configuración especifica si un usuario del dispositivo BlackBerry puede cambiar todas las reglas de política de VPN en un dispositivo BlackBerry. Si cambia el valor de esta configuración a No, un usuario puede continuar cambiando el nombre de usuario de VPN y la contraseña de VPN en un dispositivo.
Valores posibles	• Sí • No

Valor predeterminado	• Sí
Requisitos mínimos	• BlackBerry Device Software 4.0

Configuración Permitir guardar contraseña de VPN

Descripción	Esta configuración especifica si un usuario de dispositivo BlackBerry puede guardar la contraseña de VPN en un dispositivo BlackBerry.
Valores posibles	• Sí • No
Valor predeterminado	• Sí
Requisitos mínimos	• BlackBerry Device Software 4.2

Configuración Desactivar validación del certificado del servidor de VPN

Descripción	Esta configuración especifica si un dispositivo BlackBerry requiere un certificado para autenticarse en las gateways VPN que son compatibles con autenticación basada en PKI mediante certificados. Esta configuración es aplicable a las siguientes gateways VPN que son compatibles con autenticación basada en PKI mediante certificados: Cisco Secure PIX Firewall, Cisco IOS con Easy VPN Server, NetScreen Series Security Systems y Nortel Networks Contivity VPN Switch.
Valores posibles	• Sí • No
Valor predeterminado	• No
Requisitos mínimos	• BlackBerry Device Software 5.0

Configuración del DNS en la VPN

Descripción	Esta configuración especifica la configuración del DNS en la VPN de su empresa. Para requerir que un dispositivo BlackBerry recupere la configuración del DNS de la gateway de VPN, cambie esta configuración a Sí. Para requerir que el dispositivo utilice la configuración estática que se ha especificado en la configuración del DNS principal de la VPN, el DNS secundario de la VPN y el nombre de dominio de la VPN, cambie el valor a No.
Configuración relacionada	La configuración Activar VPN afecta a esta opción de configuración. Para que un dispositivo pueda utilizar esta configuración, debe configurar la opción Activar VPN en Sí.
Valores posibles	• Sí • No
Configuración predeterminada	• Sí
Requisitos mínimos	• BlackBerry Device Software 4.2

Configuración Nombre de dominio de la VPN

Descripción	Esta configuración especifica el sufijo del nombre de dominio de su empresa, en formato FQDN.
Configuración relacionada	La configuración Activar VPN afecta a esta opción de configuración. Para que un dispositivo BlackBerry pueda utilizar esta configuración, debe configurar la opción Activar VPN en Sí. La opción Configuración del DNS en la VPN afecta a esta opción de configuración. Para que el dispositivo utilice esta opción de configuración, debe configurar la opción Configuración del DNS en la VPN en No.
Valor predeterminado	• Valor nulo
Requisitos mínimos	• BlackBerry Device Software 4.2

Configuración Dirección de gateway de la VPN

Descripción	Esta configuración especifica la dirección IP o FQDN del servidor VPN de su empresa.
Valor predeterminado	• Valor nulo
Requisitos mínimos	• BlackBerry Device Software 4.2

Configuración Nombre del grupo de VPN

Descripción	Esta configuración especifica el nombre del grupo del servidor VPN de su empresa. Especifique el nombre del grupo del servidor VPN de su empresa sólo si el cliente VPN lo requiere.
Valor predeterminado	• Valor nulo
Requisitos mínimos	• BlackBerry Device Software 4.2

Configuración Contraseña del grupo de VPN

Descripción	Esta configuración especifica la contraseña del grupo del servidor VPN de su empresa. Especifique la contraseña del grupo del servidor VPN de su empresa sólo si el cliente VPN lo requiere.
Valor predeterminado	• Valor nulo
Requisitos mínimos	• BlackBerry Device Software 4.2

Configuración Identificador físico de VPN solicitado

Descripción	Esta configuración especifica si el servidor VPN requiere que un dispositivo BlackBerry utilice un identificador físico como parte de la contraseña para la autenticación.

Valores posibles	• Sí • No
Valor predeterminado	• No
Requisitos mínimos	• BlackBerry Device Software 4.2.1

Configuración Cifrado IKE de la VPN

Descripción	Esta configuración especifica el algoritmo de cifrado que un dispositivo BlackBerry utiliza para autenticar intercambios de cifrado IKE. Cambie esta configuración sólo si el algoritmo de cifrado no es compatible con AES128.
Valores posibles	• DES • 3DES • AES128 • AES192 • AES256
Valor predeterminado	• AES128
Requisitos mínimos	• BlackBerry Device Software 4.2

Configuración Grupo de claves DH del cifrado IKE de la VPN

Descripción	Esta configuración especifica el grupo de claves DH que un dispositivo BlackBerry utiliza para generar el material de clave. Cambie esta configuración sólo si el grupo de claves DH no utiliza ECC.
Configuración relacionada	La configuración Activar VPN afecta a esta regla. Para que un dispositivo pueda utilizar esta configuración, debe cambiar el valor de configuración de Activar VPN a Sí.

Valores posibles	• Grupo 1 • Grupo 2 • Grupo 5 • Grupo 7 • Grupo 9
Valor predeterminado	• Grupo 7
Requisitos mínimos	• BlackBerry Device Software 4.2

Configuración Hash del cifrado IKE de la VPN

Descripción	Esta configuración especifica el código de autenticación del método de cifrado que un dispositivo BlackBerry puede utilizar. Cambie esta configuración sólo si el código de autenticación del método de hash no es compatible con SHA1 de 160 bits.
Valores posibles	• MD5 de 128 bits • SHA1 de 160 bits
Valor predeterminado	• SHA1 de 160 bits
Requisitos mínimos	• BlackBerry Device Software 4.2

Configuración Dirección IP de VPN

Descripción	Esta configuración especifica la dirección IP de la VPN.
Valor predeterminado	• Valor nulo
Requisitos mínimos	• BlackBerry Device Software 4.2.1

Opción de configuración Cifrado y hash IPSec de la VPN

Descripción	Esta configuración especifica el algoritmo de cifrado y hash que un dispositivo BlackBerry utiliza para las asociaciones de seguridad de IPSec. Cambie esta configuración sólo si el hash de IPsec y de cifrado no son el hash SHA1 y el cifrado AES128.
Valores posibles	• Hash MD5 sin cifrado • Hash SHA1 sin cifrado • Cifrado DES sin hash • Hash MD5 y cifrado DES • Hash SHA1 y cifrado DES • Cifrado 3DES sin hash • Hash MD5 y cifrado 3DES • Hash SHA1 y cifrado 3DES • Cifrado AES128 sin hash • Hash MD5 y cifrado AES128 • Hash SHA1 y cifrado AES128 • Cifrado AES192 sin hash • Hash MD5 y cifrado AES192 • Hash SHA1 y cifrado AES192 • Cifrado AES256 sin hash • Hash MD5 y cifrado AES256 • Hash SHA1 y cifrado AES256
Valor predeterminado	• Hash SHA1 y cifrado AES128
Requisitos mínimos	• BlackBerry Device Software 4.2

Configuración Nivel mínimo de seguridad de la clave de cifrado del certificado de VPN

Descripción	Esta configuración especifica el nivel de seguridad mínimo para claves privadas que un dispositivo BlackBerry utiliza en los métodos de autenticación que requieren certificados de cliente. Si cambia el valor de esta configuración a Seguridad alta, el dispositivo solicita al usuario del dispositivo BlackBerry la contraseña del almacén de claves cada vez que el dispositivo necesite obtener acceso a la clave privada. Esto podría suceder con frecuencia, incluso si el usuario ha introducido la contraseña recientemente. Las claves privadas no se guardan con el perfil VPN. Si cambia el valor de esta configuración a Seguridad media, el dispositivo solicita al usuario la contraseña del almacén de claves la primera vez y, a partir de entonces, sólo cuando el usuario reinicia el dispositivo. Las claves privadas se guardan en memoria caché, y no con el perfil VPN. Si cambia el valor de esta configuración a Seguridad baja, el dispositivo solicita al usuario la contraseña del almacén de claves una sola vez. El dispositivo recupera y almacena en formato no cifrado la clave privada con el perfil VPN.
Valores posibles	• Seguridad baja • Seguridad alta • Seguridad media
Valor predeterminado	• Seguridad baja
Requisitos mínimos	• BlackBerry Device Software 4.2.1

Configuración Mantener activo NAT de VPN

Descripción	Esta configuración especifica la frecuencia de mantenimiento activo de NAT. Especifique el intervalo tras el cual un dispositivo BlackBerry envía un paquete de mantenimiento activo al concentrador VPN para mantener la conexión con este último.
Valores posibles	• De 1 a 1439 minutos

Valor predeterminado	• 1 minuto
Requisitos mínimos	• BlackBerry Device Software 4.2

Configuración PFS de la VPN

Descripción	Esta configuración especifica si PFS se ha activado en un dispositivo BlackBerry. Cambie esta configuración sólo si su empresa no admite PFS.
Valores posibles	• Sí • No
Valor predeterminado	• Sí
Requisitos mínimos	• BlackBerry Device Software 4.2

Configuración DNS principal de la VPN

Descripción	Este parámetro especifica la configuración estática de la dirección IP del servidor DNS principal de su empresa.
Configuración relacionada	La configuración Activar VPN afecta a esta opción de configuración. Para que un dispositivo BlackBerry pueda utilizar esta configuración, debe cambiar el valor del parámetro Activar VPN a Sí. La opción Configuración del DNS en la VPN afecta a esta opción de configuración. Para que el dispositivo utilice esta opción de configuración, debe cambiar la opción Configuración del DNS en la VPN a No.
Valor predeterminado	• Valor nulo
Requisitos mínimos	• BlackBerry Device Software 4.2

Configuración Visibilidad del perfil VPN

Descripción	Esta configuración especifica si un usuario de dispositivo BlackBerry puede ver los ajustes de configuración del perfil VPN en un dispositivo BlackBerry.
Valores posibles	• Visibilidad completa • Visibilidad limitada • Visibilidad de las credenciales
Valor predeterminado	• Visibilidad completa
Requisitos mínimos	• BlackBerry Device Software 4.2.1

Configuración Editabilidad del perfil VPN

Descripción	Esta configuración especifica si un usuario del dispositivo BlackBerry puede cambiar los ajustes de configuración del perfil VPN en un dispositivo BlackBerry.
Valores posibles	• Editabilidad completa • Sin editabilidad • Editabilidad de las credenciales
Valor predeterminado	• Editabilidad completa
Requisitos mínimos	• BlackBerry Device Software 4.2.1

Configuración DNS secundario de la VPN

Descripción	Este parámetro especifica la configuración estática de la dirección IP del servidor DNS secundario de su empresa.

Configuración relacionada	La configuración Activar VPN afecta a esta opción de configuración. Para que un dispositivo BlackBerry pueda utilizar esta configuración, debe cambiar el valor de configuración de Activar VPN a Sí. La opción Configuración del DNS en la VPN afecta a esta opción de configuración. Para que el dispositivo utilice esta opción de configuración, debe cambiar la opción Configuración del DNS en la VPN a No.
Valor predeterminado	• Valor nulo
Requisitos mínimos	• BlackBerry Device Software 4.2

Configuración Dirección IP de subred 1 de la VPN

Descripción	Esta configuración especifica la dirección IP de subred 1 para gateway de VPN que requieren que un dispositivo BlackBerry especifique una subred. Escriba la dirección IP en formato decimal con punto (por ejemplo, 192.0.2.1).
Valor predeterminado	• Valor nulo
Requisitos mínimos	• BlackBerry Device Software 4.6

Configuración Máscara de subred 1 de la VPN

Descripción	Esta configuración especifica la máscara de subred 1 para gateway de VPN que requieren que un dispositivo BlackBerry especifique una subred.
Valor predeterminado	• Valor nulo
Requisitos mínimos	• BlackBerry Device Software 4.6

Configuración Dirección IP de subred 2 de la VPN

Descripción	Esta configuración especifica la dirección IP de subred 2 para gateway de VPN que requieren que un dispositivo BlackBerry especifique una subred. Escriba la dirección IP en formato decimal con punto (por ejemplo, 192.0.2.1).
Valor predeterminado	• Valor nulo
Requisitos mínimos	• BlackBerry Device Software 4.6

Configuración Máscara de subred 2 de la VPN

Descripción	Esta configuración especifica la máscara de subred 2 para gateway de VPN que requieren que un dispositivo BlackBerry especifique una subred.
Valor predeterminado	• Valor nulo
Requisitos mínimos	• BlackBerry Device Software 4.6

Configuración Dirección IP de subred 3 de la VPN

Descripción	Esta configuración especifica la dirección IP de subred 3 para gateway de VPN que requieren que un dispositivo BlackBerry especifique una subred. Escriba la dirección IP en formato decimal con punto (por ejemplo, 192.0.2.1).
Valor predeterminado	• Valor nulo
Requisitos mínimos	• BlackBerry Device Software 4.6

Configuración Máscara de subred 3 de la VPN

Descripción	Esta configuración especifica la máscara de subred 3 para gateway de VPN que requieren que un dispositivo BlackBerry especifique una subred.
Valor predeterminado	• Valor nulo
Requisitos mínimos	• BlackBerry Device Software 4.6

Configuración Máscara de subred de la VPN

Descripción	Esta configuración especifica la dirección IP de la máscara de subred de la VPN.
Configuración relacionada	Esta opción afecta a la opción de configuración de Activar VPN. Si cambia esta configuración, debe establecer la opción Activar VPN en Sí. Esta configuración afecta a la opción Configuración del DNS en la VPN. Si cambia esta configuración, debe establecer la opción Configuración del DNS en la VPN en No.
Configuración predeterminada	• Valor nulo
Requisitos mínimos	• BlackBerry Device Software 4.2.1

Configuración Número de serie del identificador de VPN

Descripción	Si el servidor VPN requiere que un dispositivo BlackBerry utilice un identificador de software como parte de la contraseña para la autenticación, esta configuración especifica el número de serie del identificador de software que se proporciona para el dispositivo.
Valor predeterminado	• Valor nulo

Requisitos mínimos	• BlackBerry Device Software 4.2.1

Configuración Nombre de usuario de VPN

Descripción	Esta configuración especifica el nombre de usuario predeterminado que un dispositivo BlackBerry utiliza para iniciar sesión en el servidor VPN de su empresa. Configure este parámetro si desea crear un nombre de usuario predeterminado para todas las cuentas de usuario. Si un usuario de dispositivo BlackBerry introduce un nombre de usuario en un dispositivo manualmente, las actualizaciones de política de TI sobrescriben o eliminan el valor introducido por el usuario. Para conservar el valor introducido por el usuario en el dispositivo, compruebe que el valor en la configuración actualizada es el mismo que en esta configuración.
Configuración relacionada	La configuración Activar VPN afecta a esta opción de configuración. Para que un dispositivo pueda utilizar esta configuración, debe cambiar el valor de configuración de Activar VPN a Sí.
Valor predeterminado	• Valor nulo
Requisitos mínimos	• BlackBerry Device Software 4.2

Configuración Contraseña de usuario de VPN

Descripción	Esta configuración especifica la contraseña predeterminada que un dispositivo BlackBerry utiliza para iniciar sesión en el servidor VPN de su empresa. Configure este parámetro si desea crear una contraseña predeterminada para todas las cuentas de usuario. Si un usuario de dispositivo BlackBerry introduce una contraseña en un dispositivo manualmente, las actualizaciones de política de TI sobrescriben o eliminan el valor introducido por el usuario. Para conservar el valor introducido por el usuario en el dispositivo, compruebe que el valor en la configuración actualizada es el mismo que en esta configuración.
Configuración relacionada	La configuración Activar VPN afecta a esta opción de configuración. Para que un dispositivo pueda utilizar esta configuración, debe cambiar el valor de configuración de Activar VPN a Sí.
Valor predeterminado	• Valor nulo

Requisitos mínimos	• BlackBerry Device Software 4.2

Configuración Tipo de proveedor de VPN

Descripción	Esta configuración especifica el tipo de cliente VPN que el cliente VPN de un dispositivo BlackBerry emula.
Configuración relacionada	La configuración Activar VPN afecta a esta opción de configuración. Para que un dispositivo pueda utilizar esta configuración, debe configurar el valor de configuración de Activar VPN en Sí.
Valores posibles	• 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 y PowerVPN
Valor predeterminado	• Valor nulo
Requisitos mínimos	• BlackBerry Device Software 4.2

Configuración Tipo de Xauth de la VPN

Descripción	Esta configuración especifica el tipo de autenticación que los usuarios de dispositivos BlackBerry deben utilizar para el servidor VPN de su empresa.
Configuración relacionada	La configuración Activar VPN afecta a esta opción de configuración. Para que un dispositivo BlackBerry pueda utilizar esta configuración, debe cambiar el parámetro de configuración Activar VPN a Sí.
Valores posibles	• Requiere nombre de usuario y contraseña • SecurID necesaria
Valor predeterminado	• Requiere nombre de usuario y contraseña
Requisitos mínimos	• BlackBerry Device Software 4.2

Reglas de políticas de control de aplicaciones

6

Para obtener información sobre la configuración de las reglas de políticas de control de aplicaciones, consulte la *Guía de administración de BlackBerry Enterprise Server Express.*

Regla de política de control de la aplicación ¿Se permiten las conexiones de redes externas?

Descripción	Esta regla especifica si una aplicación puede realizar conexiones externas de red. Puede configurar esta regla para impedir que la aplicación envíe o reciba datos en un dispositivo BlackBerry mediante un protocolo externo (por ejemplo, WAP o TCP). También puede configurar esta regla para que una aplicación avise a un usuario de dispositivo BlackBerry antes de realizar conexiones externas a través del firewall del dispositivo.
Reglas relacionadas	Esta regla se ve afectada por la regla de política de control de aplicaciones Lista de dominios externos. La regla de política de control de aplicaciones Lista de dominios externos tiene prioridad sobre esta regla de política de control de aplicaciones.
Valores posibles	• No permitido • Permitido • Solicitar al usuario
Valor predeterminado	• Solicitar al usuario
Requisitos mínimos	• BlackBerry Device Software 4.0

Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de control de la aplicación ¿Se permiten las conexiones de redes internas?

Descripción	Esta regla especifica si una aplicación puede realizar conexiones de redes internas. Puede configurar esta regla para impedir que la aplicación envíe o reciba datos en el dispositivo BlackBerry utilizando un protocolo interno (por ejemplo, BlackBerry MDS Connection Service). También puede configurar esta regla para que una aplicación avise a un usuario de dispositivo BlackBerry antes de realizar conexiones internas a través del firewall del dispositivo.
Reglas relacionadas	Esta regla se ve afectada por la regla de política de control de aplicaciones Lista de dominios internos. La regla de política de control de aplicaciones Lista de dominios internos tiene prioridad sobre esta regla de política de control de aplicaciones.
Valores posibles	• No permitido • Permitido • Solicitar al usuario
Valor predeterminado	• Solicitar al usuario
Requisitos mínimos	• BlackBerry Device Software 4.0
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de control de la aplicación ¿Se permiten las conexiones locales?

Descripción	Esta regla especifica si una aplicación puede realizar conexiones locales de red (por ejemplo, conexiones a un dispositivo BlackBerry mediante un puerto USB o serie).
Valores posibles	• No permitido • Permitido
Valor predeterminado	• Permitido
Requisitos mínimos	• BlackBerry Device Software 4.0
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de control de la aplicación ¿Se puede modificar la configuración del dispositivo?

Descripción	Esta regla especifica si una aplicación puede cambiar las opciones de configuración y la configuración del usuario del dispositivo BlackBerry en un dispositivo BlackBerry.
Valores posibles	• No permitido • Permitido • Solicitar al usuario

Valor predeterminado	• Permitido
Requisitos mínimos	• BlackBerry Device Software 4.2.1
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de control de la aplicación ¿Se puede restablecer el contador de seguridad?

Descripción	Esta regla especifica si una aplicación puede restablecer la cantidad de tiempo que debe transcurrir para que un dispositivo BlackBerry se bloquee automáticamente.
Valores posibles	• No permitido • Permitido • Solicitar al usuario
Valor predeterminado	• No permitido
Requisitos mínimos	• BlackBerry Device Software 4.2.1
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de control de aplicaciones Mostrar información mientras bloqueado

Descripción	Esta regla especifica si una aplicación puede mostrar información en la pantalla de un dispositivo BlackBerry cuando el dispositivo está bloqueado.
Valores posibles	• No permitido • Permitido • Solicitar al usuario
Valor predeterminado	• No permitido
Requisitos mínimos	• BlackBerry 6
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP3

Regla de política de control de la aplicación Disponibilidad

Descripción	Esta regla especifica si una aplicación es opcional, necesaria o no permitida en el dispositivo BlackBerry. Puede utilizar esta regla para hacer que una aplicación específica sea obligatoria en el dispositivo o para impedir que las aplicaciones no especificadas o que no son de confianza se instalen en el dispositivo.
Valores posibles	• Opcionales • necesaria • No permitido

Valor predeterminado	• Opcionales
Requisitos mínimos	• BlackBerry Device Software 4.0
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de control de la aplicación ¿Se permite el acceso a la API de los filtros del navegador?

Descripción	Esta regla especifica si una aplicación puede acceder a las API de filtro del navegador para registrar un filtro de navegador en un dispositivo BlackBerry. Puede utilizar esta regla para permitir que las aplicaciones de terceros apliquen filtros de navegador personalizados a contenido de páginas Web en un dispositivo.
Valores posibles	• No permitido • Permitido
Valor predeterminado	• No permitido
Requisitos mínimos	• BlackBerry Device Software 4.0
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de control de aplicaciones ¿Se permite el acceso a los datos corporativos?

Descripción	Esta regla especifica si una aplicación de terceros o una aplicación complementaria desarrollada por Research In Motion puede acceder a los datos del trabajo en un dispositivo BlackBerry. Puede configurar esta regla para evitar que las aplicaciones de terceros o las aplicaciones complementarias desarrolladas por RIM accedan a los datos del trabajo de un dispositivo. El dispositivo comprueba esta regla para determinar qué aplicaciones pueden acceder a los datos del trabajo.
Valores posibles	• No permitido • Permitido
Valor predeterminado	• Permitido
Requisitos mínimos	• BlackBerry 6
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP3

Regla de política de control de la aplicación ¿Se permite el acceso a la API del correo electrónico?

Descripción	Esta regla especifica si una aplicación puede enviar y recibir mensajes de correo electrónico a través de un dispositivo BlackBerry.

Valores posibles	• No permitido • Permitido
Valor predeterminado	• Permitido
Requisitos mínimos	• BlackBerry Device Software 4.0
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de control de la aplicación ¿Se permite el acceso a la API de inyección de eventos?

Descripción	Esta regla especifica si una aplicación puede simular eventos de entrada en un dispositivo BlackBerry, como pulsar teclas o realizar acciones de la bola de desplazamiento.
Valores posibles	• No permitido • Permitido
Valor predeterminado	• Permitido
Requisitos mínimos	• BlackBerry Device Software 4.0
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de control de la aplicación ¿Se permite el acceso a la API de archivo?

Descripción	Esta regla especifica si una aplicación puede cambiar, eliminar, mover o acceder a los archivos de un dispositivo BlackBerry.
Valores posibles	• No permitido • Permitido
Valor predeterminado	• Permitido
Requisitos mínimos	• BlackBerry Device Software 4.2
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de control de la aplicación ¿Se permite el acceso a la API del GPS?

Descripción	Esta regla especifica si una aplicación puede acceder a las API del GPS en un dispositivo BlackBerry. Puede configurar esta regla para impedir que la aplicación acceda a las API de GPS en un dispositivo o para enviar una solicitud al usuario del dispositivo BlackBerry para que una aplicación pueda acceder a las API del GPS.
Valores posibles	• No permitido • Permitido • Solicitar al usuario

Valor predeterminado	• Solicitar al usuario
Requisitos mínimos	• BlackBerry Device Software 4.0
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de control de la aplicación ¿Se permite el acceso al almacén de claves del dispositivo?

Descripción	Esta regla especifica si una aplicación puede obtener acceso a las API del almacén de claves en un dispositivo BlackBerry.
Valores posibles	• No permitido • Permitido
Valor predeterminado	• Permitido
Requisitos mínimos	• BlackBerry Device Software 4.0
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de control de la aplicación ¿Se permite el acceso a la API de comunicación entre procesos?

Descripción	Esta regla especifica si una aplicación puede realizar operaciones de comunicación cruzada entre aplicaciones. Puede utilizar esta regla para permitir que dos o más aplicaciones compartan datos o que una aplicación utilice los permisos de conexión de otra aplicación.
Valores posibles	• No permitido • Permitido
Valor predeterminado	• Permitido
Requisitos mínimos	• BlackBerry Device Software 4.0
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de control de la aplicación ¿Se permite el acceso a la API multimedia?

Descripción	Esta regla especifica si una aplicación puede ejecutar o crear archivos multimedia en un dispositivo BlackBerry.
Valores posibles	• No permitido • Permitido

Valor predeterminado	• Permitido
Requisitos mínimos	• BlackBerry Device Software 4.3
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de control de la aplicación ¿Se permite el acceso a la API de gestión del módulo?

Descripción	Esta regla especifica si una aplicación puede agregar, modificar o eliminar archivos .cod de Java en el dispositivo BlackBerry.
Valores posibles	• No permitido • Permitido
Valor predeterminado	• Permitido
Requisitos mínimos	• BlackBerry Device Software 4.3
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de control de la aplicación ¿Se permite el acceso al protocolo Near Field Communication (NFC)?

Descripción	Esta regla especifica si una aplicación puede acceder a NFC en el dispositivo BlackBerry.
Valores posibles	• No permitido • Permitido • Solicitar al usuario
Valor predeterminado	• Permitido
Requisitos mínimos	• BlackBerry 7
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP4

Regla de política de control de la aplicación ¿Se permite el acceso a la API del PIM?

Descripción	Esta regla especifica si una aplicación puede acceder a las API del PIM del dispositivo BlackBerry, que controlan el acceso a la información personal del usuario del dispositivo BlackBerry, como los contactos, en un dispositivo. Si permite a una aplicación acceder a las API de los datos del PIM y utilizar los protocolos de conexión de red, la aplicación podría enviar toda la información personal del usuario desde el dispositivo.
Valores posibles	• No permitido

	• Permitido
Valor predeterminado	• Permitido
Requisitos mínimos	• BlackBerry Device Software 4.0
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de control de la aplicación ¿Se permite el acceso a la API del teléfono?

Descripción	Esta regla especifica si una aplicación puede hacer llamadas, responder a llamadas entrantes y acceder a registros de llamadas en un dispositivo BlackBerry. Puede configurar esta regla para impedir que la aplicación realice llamadas en un dispositivo o para solicitar al usuario de un dispositivo BlackBerry que permita las llamadas antes de que la aplicación las realice.
Valores posibles	• No permitido • Permitido • Solicitar al usuario
Valor predeterminado	• Solicitar al usuario
Requisitos mínimos	• BlackBerry Device Software 4.0
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de control de la aplicación ¿Se permite el acceso a la pantalla, el micrófono y las API de captura de vídeo?

Descripción	Esta regla especifica si una aplicación puede grabar contenido multimedia, como audio y vídeo, utilizando BlackBerry Browser u otras aplicaciones en un dispositivo BlackBerry.
Valores posibles	• No permitido • Permitido • Solicitar al usuario
Valor predeterminado	• No permitido
Requisitos mínimos	• BlackBerry Device Software 4.2.1
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de control de la aplicación ¿Se permite el acceso al elemento seguro?

Descripción	Esta regla especifica si una aplicación puede acceder al elemento seguro en el dispositivo BlackBerry.
Valores posibles	• No permitido • Permitido • Solicitar al usuario

Valor predeterminado	• Permitido
Requisitos mínimos	• BlackBerry 7
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP4

Regla de política de control de la aplicación ¿Se permite el acceso al perfil de puerto de serie para la API de Bluetooth?

Descripción	Esta regla especifica si una aplicación puede acceder a la API del SSP Bluetooth®.
Valores posibles	• No permitido • Permitido
Valor predeterminado	• Permitido
Requisitos mínimos	• BlackBerry Device Software 4.0
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de control de la aplicación ¿Se permite el acceso a la API del autenticador del usuario?

Descripción	Esta regla especifica si una aplicación puede obtener acceso a la API del marco de autenticación del usuario. El marco de autenticación del usuario permite el registro de controladores que ofrecen autenticación de dos factores para desbloquear un dispositivo BlackBerry. Esta regla se aplica a BlackBerry Device Software y a las aplicaciones Java de terceros. Para dispositivos que ejecutan BlackBerry Device Software 5.0 y posterior, esta regla se aplica a los controladores de lectores de tarjetas inteligentes y a los métodos de autenticación de dos factores personalizados creados por los desarrolladores de la empresa. Para dispositivos que ejecutan BlackBerry Device Software 4.7 y anterior, esta regla se aplica únicamente a los controladores de tarjetas inteligentes.
Valores posibles	• No permitido • Permitido
Valor predeterminado	• Permitido
Requisitos mínimos	• BlackBerry Device Software 4.0
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de control de la aplicación ¿Se permite el acceso a la API de Wi-Fi?

Descripción	Esta regla especifica si una aplicación en un dispositivo BlackBerry puede enviar y recibir datos a través de una conexión Wi-Fi y acceder a la información sobre la red Wi-Fi.
Valores posibles	• No permitido • Permitido • Solicitar al usuario
Valor predeterminado	• Solicitar al usuario
Requisitos mínimos	• BlackBerry Device Software 4.2.1
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de control de la aplicación ¿Se permite la seguridad de medios del almacén de claves?

Descripción	Esta regla especifica si una aplicación puede acceder a los elementos del almacén de claves que tienen un nivel de seguridad medio. La aplicación debe solicitar a un usuario de dispositivo BlackBerry la contraseña del almacén de claves cuando intenta acceder a la clave privada por primera vez o cuando el tiempo de espera de la contraseña de clave privada se agota.
Valores posibles	• No permitido

	• Permitido
Valor predeterminado	• Permitido
Requisitos mínimos	• BlackBerry Device Software 4.0
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de control de aplicaciones ¿Se permite la gestión de conexiones?

Descripción	Esta regla especifica si una aplicación puede gestionar conexiones e información relacionada con las mismas en un dispositivo BlackBerry.
Valores posibles	• No permitido • Permitido
Valor predeterminado	• Permitido
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP3

Regla de política de control de aplicaciones ¿Se permite el control multimedia?

Descripción	Esta regla especifica si una aplicación puede abrir o gestionar archivos multimedia en un dispositivo BlackBerry.

Valores posibles	• No permitido • Permitido • Solicitar al usuario
Valor predeterminado	• Permitido
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP3

Regla de política de control de la aplicación ¿Se permiten los datos de tema?

Descripción	Esta regla especifica si un usuario del dispositivo BlackBerry puede utilizar como temas las aplicaciones de temas personalizados desarrolladas mediante Plazmic Content Developer's Kit en un dispositivo BlackBerry.
Valores posibles	• No permitido • Permitido
Valor predeterminado	• Permitido
Requisitos mínimos	• BlackBerry Device Software 4.0
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de control de la aplicación Lista de dominios del filtro del navegador

Descripción	Esta regla especifica la lista de dominios en los que una aplicación puede aplicar filtros de navegador al contenido de una página Web en un dispositivo BlackBerry. Por ejemplo, puede especificar www.google.com y www.yahoo.com como dominios para los cuales una aplicación puede utilizar un filtro del navegador para motores de búsqueda.
Valor predeterminado	• Valor nulo
Requisitos mínimos	• BlackBerry Device Software 4.0
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de control de la aplicación Lista de dominios externos

Descripción	Esta regla especifica los nombres de dominio externos con los que una aplicación puede establecer una conexión. Esta regla no admite caracteres comodín. Separe los dominios diferentes con un punto y coma (;). Puede configurar esta regla de política de control de aplicaciones y una regla de extracción que BlackBerry MDS Connection Service utilizará para controlar si un usuario de dispositivo BlackBerry puede acceder a un dominio externo. Si configura esta regla y una regla de extracción para un dominio externo, el usuario no podrá acceder al dominio externo a menos que esta regla y la regla de extracción permitan el acceso.
Reglas relacionadas	Esta regla afectará a la regla de política de control de aplicaciones ¿Se permiten las conexiones de redes externas? La aplicación en un dispositivo BlackBerry se puede conectar a los dominios que

	especifique en esta regla, incluso si configura la regla de política de control de aplicaciones ¿Se permiten las conexiones de redes externas? en No permitido.
Valor predeterminado	• Valor nulo
Requisitos mínimos	• BlackBerry Device Software 4.0
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Regla de política de control de la aplicación Lista de dominios internos

Descripción	Esta regla especifica los nombres de dominio internos con los que una aplicación puede establecer una conexión. Esta regla no admite caracteres comodín. Separe los dominios diferentes con un punto y coma (;).
Reglas relacionadas	Esta regla afectará a la regla de política de control de aplicaciones ¿Se permiten las conexiones de redes internas? La aplicación en un dispositivo BlackBerry se puede conectar a los dominios que especifique en esta regla, incluso si configura la regla de política de control de aplicaciones ¿Se permiten las conexiones de redes internas? en No permitido.
Valor predeterminado	• Valor nulo
Requisitos mínimos	• BlackBerry Device Software 4.0
Introducción a las reglas	• BlackBerry Enterprise Server Express 5.0 SP1

Ejemplos de objetivos de la política de seguridad

7

Requisito del uso de una contraseña en un dispositivo

Situación	Regla de política de TI	Grupo de políticas de IT	Valor
Amplíe la política de contraseñas de su empresa a los dispositivos BlackBerry.	Contraseña necesaria	Grupo de políticas de Sólo dispositivo	Sí
	Tiempo máximo de validez de la contraseña	Grupo de políticas de Sólo dispositivo	30
	Longitud mínima de la contraseña	Grupo de políticas de Sólo dispositivo	8
	Comprobaciones de patrones de contraseña	Grupo de políticas de Sólo dispositivo	Al menos 1 carácter alfabético, 1 carácter numérico y 1 carácter especial
	Definir el tiempo de espera de contraseña	Grupo de políticas de contraseña	5
	El usuario puede modificar el tiempo de espera	Grupo de políticas de Sólo dispositivo	No
Elimine todos los datos de usuario del dispositivo si el usuario de un dispositivo BlackBerry escribe la contraseña incorrectamente.	Definir los intentos máximos de contraseña	Grupo de políticas de contraseña	10

Situación	Regla de política de TI	Grupo de políticas de IT	Valor
No permitir que el usuario vuelva a emplear una contraseña caducada.	Historial máximo de contraseñas	Grupo de políticas de contraseña	10

Evitar el uso no autorizado de un dispositivo

Situación	Regla de política de TI	Grupo de políticas	Valor
Bloquear el dispositivo BlackBerry automáticamente, independientemente de la actividad del usuario.	Activar el tiempo de espera a largo plazo	Grupo de políticas de Sólo dispositivo	Sí
Solicitar al usuario del dispositivo BlackBerry que escriba la contraseña periódicamente.	Tiempo periódico de búsqueda	Grupo de políticas de contraseña	60
Bloquear el dispositivo automáticamente tras un período de inactividad del usuario.	Tiempo de espera de seguridad máximo	Grupo de políticas de Sólo dispositivo	10

Cifrar los datos en un dispositivo

Situación	Regla de política de TI	Grupo de políticas	Valor
Proteja los datos del usuario del dispositivo BlackBerry y los datos de aplicaciones en el dispositivo BlackBerry.	Intensidad de protección de contenido	Seguridad	Extremadamente alta
Especifique los algoritmos que el dispositivo utiliza para cifrar y descifrar los mensajes PGP.	Cifrados de contenido PGP permitido	Aplicación PGP	AES (256 bits), AES (192 bits), AES (128 bits) y Triple DES

Situación	Regla de política de TI	Grupo de políticas	Valor
Especifique los algoritmos que el dispositivo utiliza para cifrar y descifrar los mensajes S/MIME.	Cifrados de contenido S/MIME permitido	Aplicación S/MIME	AES (256 bits), AES (192 bits), AES (128 bits) y Triple DES

Restringir la mensajería en un dispositivo

Situación	Regla de política de TI	Grupo de políticas	Valor
Restringir la mensajería en un dispositivo BlackBerry a los servicios de mensajería que su empresa puede controlar.	Permitir otros servicios del navegador	Exclusividad del servicio	No
	Permitir otros servicios de mensajes	Exclusividad del servicio	No
	Permitir la mensajería "punto a punto"	Sólo dispositivo	No
	Permitir SMS	Sólo dispositivo	No
	Desactivar el reenvío entre los servicios	Seguridad	Sí
	Desactivar cortar/copiar/pegar	Seguridad	Sí
Solicitar al usuario del dispositivo BlackBerry que envíe los mensajes de correo electrónico cifrados desde el dispositivo.	S/MIME fuerza los mensajes cifrados	Aplicación S/MIME	Sí
	PGP fuerza los mensajes cifrados	Aplicación PGP	Sí
Evitar que el usuario envíe mensajes PIN.	Permitir la mensajería "punto a punto"	Sólo dispositivo	No
Evitar que el usuario envíe mensajes de texto SMS.	Permitir SMS	Sólo dispositivo	No
Evitar que el usuario reenvíe o responda a mensajes de correo electrónico a través de diferentes servicios de mensajería.	Desactivar el reenvío entre los servicios	Seguridad	Sí

Definir las medidas para evitar las amenazas de virus y usuarios malintencionados

Considere utilizar las reglas de política de TI y las reglas de política de control de aplicaciones para bloquear las amenazas de virus y otros métodos del ataque de usuarios malintencionados.

Limitar los recursos a los que una aplicación de terceros puede acceder en un dispositivo

Situación	Ejemplo de reglas de política de control de la aplicación	Valor
Evitar que aplicaciones Java de terceros accedan a una lista de dominios con BlackBerry Browser.	Lista de dominios del filtro del navegador	direcciones de los dominios
Permitir a una aplicación Java de terceros enviar y recibir mensajes en un dispositivo BlackBerry.	¿Se permite el acceso a la API del correo electrónico?	Permitido
Eliminar una aplicación Java de terceros de dispositivos BlackBerry a través de la red inalámbrica.	Disponibilidad	No permitido
Permitir a una aplicación Java de terceros acceder a la aplicación de teléfono en dispositivos BlackBerry.	¿Se permite el acceso a la API del teléfono?	Permitido
Permitir que una aplicación Java de terceros cree conexiones externas públicas de red y autorice conexiones a dominios externos sin solicitar la contraseña a los usuarios de dispositivos BlackBerry.	¿Se permiten las conexiones de redes externas?	Permitido
	Lista de dominios externos	direcciones de los dominios externos
Permitir que una aplicación Java de terceros establezca conexiones con dispositivos con Bluetooth.	¿Se permite el acceso al perfil de puerto de serie para la API de Bluetooth?	Permitido

Situación	Ejemplo de reglas de política de control de la aplicación	Valor
	¿Se permiten las conexiones de redes externas?	Permitido
Impedir que los usuarios activen un tema personalizado creado mediante Plazmic Content Developer's Kit.	¿Se permiten los datos de tema?	No permitido
Impedir que los usuarios desbloqueen sus dispositivos BlackBerry mediante un BlackBerry Smart Card Reader y una contraseña de autenticación.	¿Se permite el acceso a la API del autenticador del usuario?	No permitido

Limitación del control del usuario sobre aplicaciones de terceros en dispositivos BlackBerry

Situación	Ejemplo de regla de política	Valor
Impedir que las aplicaciones de terceros obtengan acceso a los puertos serie o puertos USB en dispositivos BlackBerry.	Permitir que aplicaciones de terceros usen el puerto serie, regla de política de TI	No
Impedir que los usuarios descarguen aplicaciones o temas de terceros en sus dispositivos BlackBerry.	Desactivar la descarga de aplicaciones de otros fabricantes, regla de política de TI	Sí
Impedir que los usuarios eliminen una aplicación Java de terceros instalada en sus dispositivos BlackBerry.	Disponibilidad, regla de política de control de la aplicación	Necesarias
Impedir que los usuarios instalen una aplicación Java de terceros sus dispositivos BlackBerry.	Disponibilidad, regla de política de control de la aplicación	No permitido
Eliminar una aplicación Java de terceros de dispositivos BlackBerry a través de la red inalámbrica.	Disponibilidad, regla de política de control de la aplicación	No permitido
Impedir que los usuarios activen un tema personalizado creado mediante BlackBerry Theme Studio.	¿Se permiten los datos de tema? (regla de política de control de la aplicación)	Necesarias
Impedir que los usuarios desbloqueen sus dispositivos BlackBerry mediante un BlackBerry	¿Se permite el acceso a la API del autenticador del usuario?	Necesarias

Situación	Ejemplo de regla de política	Valor
Smart Card Reader y una contraseña de autenticación.	(regla de política de control de la aplicación)	
Impedir que los usuarios que se van a autenticar a través de una conexión VPN utilicen aplicaciones de terceros en sus dispositivos BlackBerry.	¿Se permite el acceso a la API del autenticador del usuario? (regla de política de control de la aplicación)	Necesarias

Cómo evitar que las aplicaciones de valor añadido de RIM se ejecuten en dispositivos BlackBerry

Puede utilizar las reglas de política de control de la aplicación y las reglas de política de TI para controlar si las aplicaciones de valor añadido de Research In Motion están disponibles en los dispositivos BlackBerry. Las aplicaciones de valor añadido de RIM incluyen BlackBerry Wallet y E-Commerce Content Optimization Engine para BlackBerry Browser.

Para impedir que las aplicaciones de valor añadido de RIM se ejecuten en versiones de BlackBerry Device Software anteriores a la versión 4.5, puede bloquear todas las aplicaciones de valor añadido de RIM mediante la regla de política de TI Desactivar aplicaciones de valor añadido de RIM o puede bloquear las aplicaciones específicas de valor añadido de RIM mediante las reglas de política de TI específicas de la aplicación.

Para impedir que las aplicaciones de valor añadido de RIM se ejecuten en BlackBerry Device Software versión 4.5 o posterior, puede utilizar cualquiera de los siguientes métodos específicos de la aplicación:

Descripción general	Método
BlackBerry Wallet	• Configure la regla de política de TI Desactivar BlackBerry Wallet en Sí. • Aplique una regla de política de control de una aplicación para bloquear todas las aplicaciones de terceros, o aplique una política de control de la aplicación para bloquear las aplicaciones específicas de valor añadido de RIM si desea eliminarlas de los dispositivos BlackBerry. • Configure la regla de política de TI Desactivar aplicaciones de valor añadido de RIM en Sí.
E-Commerce Content Optimization Engine (motor para optimización de contenido en comercio electrónico) para BlackBerry Browser	• Configure la regla de política de TI Desactivar E-Commerce Content Optimization Engine (motor para optimización de contenido en comercio electrónico) en Sí.

Descripción general	Método
	• Aplique una regla de política de control de la aplicación para bloquear todas las aplicaciones de terceros, o aplique una política de control de la aplicación para bloquear las aplicaciones específicas de valor añadido de RIM si desea eliminarlas de los dispositivos BlackBerry. • Configure la regla de política de TI Desactivar aplicaciones de valor añadido de RIM en Sí.

Puede aplicar la regla de política de control de la aplicación Disponibilidad a aplicaciones de valor añadido de RIM únicamente. Otras reglas de política de control de la aplicación no se aplican a aplicaciones de valor añadido de RIM.

Glosario

8

AES	Advanced Encryption Standard (Estándar de cifrado avanzado)
API	Application Programming Interface (Interfaz de programación de aplicaciones)
BIP	Protocolo BIP
CAST	Computer Assisted Seriation Test (Prueba de seriación asistida por ordenador)
DES	Data Encryption Standard (Estándar de cifrado de datos)
DH	Diffie-Hellman
DSA	Digital Signature Algorithm (Algoritmo de firma digital)
EAP-LEAP	Extensible Authentication Protocol Lightweight Extensible Authentication Protocol (Protocolo de autenticación extensible Protocolo ligero de autenticación extensible)
ECC	Elliptic Curve Cryptography (Criptografía de curva elíptica)
FTP	File Transfer Protocol (Protocolo de transferencia de archivos)
sobre de mensaje de gateway	El protocolo GME (Gateway Message Envelope, Sobre de mensaje de gateway) es un protocolo propio de Research In Motion que permite la transferencia de datos comprimidos y cifrados entre la red inalámbrica y dispositivos BlackBerry. El protocolo define una capa de enrutamiento que especifica los tipos de contenido del mensaje permitidos y la información de direccionamiento de los datos. Los gateways y componentes de enrutamiento utilizan esta información para identificar el tipo y el origen de los datos del dispositivo BlackBerry y el servicio de destino apropiado al que enrutar los datos.
GPS	Global Positioning System (Sistema de posicionamiento global)
HTML	Hypertext Markup Language (Lenguaje de marcadores de hipertexto)
IP	Internet Protocol (Protocolo de Internet)
TI	information technology (tecnología de la información)
MFH	message from handheld (mensaje del dispositivo)
MMS	Multimedia Messaging Service (Servicio de mensajería multimedia)
MTH	message to handheld (mensaje para el dispositivo)
NFC	Near Field Communication
PIM	personal information management (administración de información personal)

PIN	personal identification number (número de identificación personal)
RC	Rivest's Cipher (Cifrado Rivest)
S/MIME	Secure Multipurpose Internet Mail Extensions (Extensiones seguras multiuso del correo de Internet)
SMS	Short Message Service (Servicio de mensajes cortos)
SPP	Perfil de puerto serie
TCP	Transmission Control Protocol (Protocolo de control de transmisión)
USB	Universal Serial Bus (Bus de serie universal)
VPN	virtual private network (red privada virtual)
WAN	wide area network (red de área extensa)
WAP	Wireless Application Protocol (Protocolo de aplicaciones inalámbricas)
xAuth	Autenticación ampliada

Aviso legal

9

©2012 Research In Motion Limited. Reservados todos los derechos. BlackBerry®, RIM®, Research In Motion® y las marcas comerciales, nombres y logotipos relacionados son propiedad de Research In Motion Limited y están registrados y/o se utilizan en EE. UU. y en diferentes países del mundo.

Bluetooth es una marca comercial de Bluetooth SIG. Entrust y Entrust Entelligence son marcas comerciales de Entrust, Inc. IrDA es una marca comercial de Infrared Data Association. PGP es una marca comercial de PGP Corporation. Plazmic es una marca comercial de Plazmic, Inc. Roxio es una marca comercial de Sonic Solutions. RSA y RSA SecurID son marcas comerciales de RSA Security. IBM, Domino, Lotus y Lotus Notes son marcas comerciales de International Business Machines Corporation. Java y JavaScript son marcas comerciales de Oracle America, Inc. Wi-Fi es una marca comercial de Wi-Fi Alliance. Todas las demás marcas comerciales son propiedad de sus respectivos propietarios.

Esta documentación, incluida cualquier documentación que se incorpore mediante referencia como documento proporcionado o disponible en www.blackberry.com/go/docs, se proporciona o se pone a disposición "TAL CUAL" y "SEGÚN SU DISPONIBILIDAD" sin ninguna condición, responsabilidad o garantía de ningún tipo por Research In Motion Limited y sus empresas afiliadas ("RIM") y RIM no asume ninguna responsabilidad por los errores tipográficos, técnicos o cualquier otra imprecisión, error u omisión contenidos en esta documentación. Con el fin de proteger la información confidencial y propia de RIM, así como los secretos comerciales, la presente documentación describe algunos aspectos de la tecnología de RIM en líneas generales. RIM se reserva el derecho a modificar periódicamente la información que contiene esta documentación, si bien tampoco se compromete en modo alguno a proporcionar cambios, actualizaciones, ampliaciones o cualquier otro tipo de información que se pueda agregar a esta documentación.

Esta documentación puede contener referencias a fuentes de información, hardware o software, productos o servicios, incluidos componentes y contenido como, por ejemplo, el contenido protegido por copyright y/o sitios Web de terceros (conjuntamente, los "Productos y servicios de terceros"). RIM no controla ni es responsable de ningún tipo de Productos y servicios de terceros, incluido, sin restricciones, el contenido, la exactitud, el cumplimiento de copyright, la compatibilidad, el rendimiento, la honradez, la legalidad, la decencia, los vínculos o cualquier otro aspecto de los Productos y servicios de terceros. La inclusión de una referencia a los Productos y servicios de terceros en esta documentación no implica que RIM se haga responsable de dichos Productos y servicios de terceros o de dichos terceros en modo alguno.

EXCEPTO EN LA MEDIDA EN QUE LO PROHÍBA ESPECÍFICAMENTE LA LEY DE SU JURISDICCIÓN, QUEDAN EXCLUIDAS POR LA PRESENTE TODAS LAS CONDICIONES, APROBACIONES O GARANTÍAS DE CUALQUIER TIPO, EXPLÍCITAS O IMPLÍCITAS, INCLUIDA, SIN NINGÚN TIPO DE LIMITACIÓN, CUALQUIER CONDICIÓN, APROBACIÓN, GARANTÍA, DECLARACIÓN DE GARANTÍA DE DURABILIDAD, IDONEIDAD PARA UN FIN O USO DETERMINADO, COMERCIABILIDAD, CALIDAD COMERCIAL, ESTADO DE NO INFRACCIÓN, CALIDAD SATISFACTORIA O TITULARIDAD, O QUE SE DERIVE DE UNA LEY O COSTUMBRE O UN CURSO DE LAS NEGOCIACIONES O USO DEL COMERCIO, O RELACIONADO CON LA DOCUMENTACIÓN O SU USO O RENDIMIENTO O NO RENDIMIENTO DE CUALQUIER SOFTWARE, HARDWARE, SERVICIO O CUALQUIER PRODUCTO O SERVICIO DE TERCEROS MENCIONADOS AQUÍ. TAMBIÉN PODRÍA TENER OTROS DERECHOS QUE VARÍAN SEGÚN EL ESTADO O PROVINCIA. ES POSIBLE QUE ALGUNAS JURISDICCIONES NO PERMITAN LA EXCLUSIÓN O LA LIMITACIÓN DE GARANTÍAS IMPLÍCITAS Y CONDICIONES. EN LA MEDIDA EN QUE LO PERMITA LA LEY, CUALQUIER GARANTÍA IMPLÍCITA O CONDICIONES EN RELACIÓN CON LA DOCUMENTACIÓN NO SE

PUEDEN EXCLUIR TAL Y COMO SE HA EXPUESTO ANTERIORMENTE, PERO PUEDEN SER LIMITADAS, Y POR LA PRESENTE ESTÁN LIMITADAS A NOVENTA (90) DÍAS DESDE DE LA FECHA QUE ADQUIRIÓ LA DOCUMENTACIÓN O EL ELEMENTO QUE ES SUJETO DE LA RECLAMACIÓN.

EN LA MEDIDA MÁXIMA EN QUE LO PERMITA LA LEY DE SU JURISDICCIÓN, EN NINGÚN CASO RIM ASUMIRÁ RESPONSABILIDAD ALGUNA POR CUALQUIER TIPO DE DAÑOS RELACIONADOS CON ESTA DOCUMENTACIÓN O SU USO, O RENDIMIENTO O NO RENDIMIENTO DE CUALQUIER SOFTWARE, HARDWARE, SERVICIO O PRODUCTOS Y SERVICIOS DE TERCEROS AQUÍ MENCIONADOS INCLUIDOS SIN NINGÚN TIPO DE LIMITACIÓN CUALQUIERA DE LOS SIGUIENTES DAÑOS: DIRECTOS, RESULTANTES, EJEMPLARES, INCIDENTALES, INDIRECTOS, ESPECIALES, PUNITIVOS O AGRAVADOS, DAÑOS POR PÉRDIDA DE BENEFICIOS O INGRESOS, IMPOSIBILIDAD DE CONSEGUIR LOS AHORROS ESPERADOS, INTERRUPCIÓN DE LA ACTIVIDAD COMERCIAL, PÉRDIDA DE INFORMACIÓN COMERCIAL, PÉRDIDA DE LA OPORTUNIDAD DE NEGOCIO O CORRUPCIÓN O PÉRDIDA DE DATOS, IMPOSIBILIDAD DE TRANSMITIR O RECIBIR CUALQUIER DATO, PROBLEMAS ASOCIADOS CON CUALQUIER APLICACIÓN QUE SE UTILICE JUNTO CON PRODUCTOS Y SERVICIOS DE RIM, COSTES DEBIDOS AL TIEMPO DE INACTIVIDAD, PÉRDIDA DE USO DE LOS PRODUCTOS Y SERVICIOS DE RIM O PARTE DE ÉL O DE CUALQUIER SERVICIO DE USO, COSTE DE SERVICIOS SUSTITUTIVOS, COSTES DE COBERTURA, INSTALACIONES O SERVICIOS, COSTE DEL CAPITAL O CUALQUIER OTRA PÉRDIDA MONETARIA SIMILAR, TANTO SI DICHOS DAÑOS SE HAN PREVISTO O NO, Y AUNQUE SE HAYA AVISADO A RIM DE LA POSIBILIDAD DE DICHOS DAÑOS.

EN LA MEDIDA MÁXIMA EN QUE LO PERMITA LA LEY DE SU JURISDICCIÓN, RIM NO TENDRÁ NINGÚN OTRO TIPO DE OBLIGACIÓN O RESPONSABILIDAD CONTRACTUAL, EXTRACONTRACTUAL O CUALQUIER OTRA, INCLUIDA CUALQUIER RESPONSABILIDAD POR NEGLIGENCIA O RESPONSABILIDAD ESTRICTA.

LAS LIMITACIONES, EXCLUSIONES Y DESCARGOS DE RESPONSABILIDAD SE APLICARÁN: (A) INDEPENDIENTEMENTE DE LA NATURALEZA DE LA CAUSA DE LA ACCIÓN, DEMANDA O ACCIÓN SUYA, INCLUIDA PERO NO LIMITADA AL INCUMPLIMIENTO DEL CONTRATO, NEGLIGENCIA, AGRAVIO, EXTRACONTRACTUAL, RESPONSABILIDAD ESTRICTA O CUALQUIER OTRA TEORÍA DEL DERECHO Y DEBERÁN SOBREVIVIR A UNO O MÁS INCUMPLIMIENTOS ESENCIALES O AL INCUMPLIMIENTO DEL PROPÓSITO ESENCIAL DE ESTE CONTRATO O CUALQUIER SOLUCIÓN CONTENIDA AQUÍ; Y (B) A RIM Y A SUS EMPRESAS AFILIADAS, SUS SUCESORES, CESIONARIOS, AGENTES, PROVEEDORES (INCLUIDOS LOS PROVEEDORES DE SERVICIOS DE USO), DISTRIBUIDORES AUTORIZADOS POR RIM (INCLUIDOS TAMBIÉN LOS PROVEEDORES DE SERVICIOS DE USO) Y SUS RESPECTIVOS DIRECTORES, EMPLEADOS Y CONTRATISTAS INDEPENDIENTES.

ADEMÁS DE LAS LIMITACIONES Y EXCLUSIONES MENCIONADAS ANTERIORMENTE, EN NINGÚN CASO NINGÚN DIRECTOR, EMPLEADO, AGENTE, DISTRIBUIDOR, PROVEEDOR, CONTRATISTA INDEPENDIENTE DE RIM O CUALQUIER AFILIADO DE RIM ASUMIRÁ NINGUNA RESPONSABILIDAD DERIVADA DE O RELACIONADA CON LA DOCUMENTACIÓN.

Antes de instalar, usar o suscribirse a cualquiera de los Productos y servicios de terceros, es su responsabilidad asegurarse de que su proveedor de servicios de uso ofrezca compatibilidad con todas sus funciones. Puede que algunos proveedores de servicios de uso no ofrezcan las funciones de exploración de Internet con una suscripción al servicio BlackBerry® Internet Service. Consulte con su proveedor de servicios acerca de la disponibilidad, arreglos de itinerancia, planes de servicio y funciones. La instalación o el uso de los Productos y servicios de terceros con productos y servicios de RIM puede precisar la obtención de una o más patentes, marcas comerciales, derechos de autor u otras licencias para evitar que se vulneren o violen derechos de terceros. Usted es el único responsable de determinar si desea utilizar Productos y servicios de terceros y si se necesita para ello cualquier otra licencia de terceros. En caso de necesitarlas, usted es el único responsable de su adquisición. No instale o utilice Productos y servicios de terceros hasta que se hayan adquirido todas las licencias necesarias. Cualquier tipo de Productos y servicios de terceros que se proporcione con los productos y servicios

de RIM se le facilita para su comodidad "TAL CUAL" sin ninguna condición expresa e implícita, aprobación, garantía de cualquier tipo por RIM y RIM no sume ninguna responsabilidad en relación con ello. El uso de los Productos y servicios de terceros se regirá y estará sujeto a la aceptación de los términos de licencias independientes aplicables en este caso con terceros, excepto en los casos cubiertos expresamente por una licencia u otro acuerdo con RIM.

Algunas funciones mencionadas en esta documentación requieren una versión mínima del software de BlackBerry® Enterprise Server, BlackBerry® Desktop Software y/o BlackBerry® Device Software.

Los términos de uso de cualquier producto o servicio de RIM se presentan en una licencia independiente o en otro acuerdo con RIM que se aplica en este caso. NINGUNA PARTE DE LA PRESENTE DOCUMENTACIÓN ESTÁ PENSADA PARA PREVALECER SOBRE CUALQUIER ACUERDO EXPRESO POR ESCRITO O GARANTÍA PROPORCIONADA POR RIM PARA PARTES DE CUALQUIER PRODUCTO O SERVICIO DE RIM QUE NO SEA ESTA DOCUMENTACIÓN.

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

Research In Motion UK Limited
Centrum House
36 Station Road
Egham, Surrey TW20 9LF
Reino Unido

Publicado en Canadá