BlackBerry UEM

Guía de administración

12.10

Contents

Pasos para comenzar a utilizar BlackBerry UEM..... 13

Características compatibles por tipo de dispositivo.....14
Gestión de aplicaciones de BlackBerry Dynamics en BlackBerry UEM..... 22
Dispositivos BlackBerry con Android.....23
Opciones de gestión de dispositivos..... 23
Administración de dispositivos que no sean smartphones, tabletas y portátiles.....23
Gestión de los dispositivos accesorios..... 24
Gestionar dispositivos Apple TV.....24
¿En qué consiste BlackBerry UEM Client ?.....25
¿En qué consiste BlackBerry UEM Self-Service ?.....27
Servicios de BlackBerry Enterprise Mobility Suite.....27
Inicio de sesión en BlackBerry UEM.....29

Wi-Fi, VPN, BlackBerry Secure Connect Plus y otras conexiones de trabajo....30

Pasos para configurar las conexiones de trabajo para dispositivos.....30
Procedimiento recomendado: creación de perfiles de conexión de trabajo.....30
Configuración de las redes Wi-Fi de trabajo para dispositivos.....31
Creación de un perfil de Wi-Fi..... 31
Configuración de las VPN de trabajo para dispositivos.....32
Crear un perfil VPN.....33
Activación de VPN a petición para dispositivos iOS o macOS.....34
Activación de una VPN por aplicación..... 34
Configuración de los perfiles de proxy para dispositivos.....35
Creación de un perfil de proxy..... 37
Uso de la conectividad de la empresa y BlackBerry Secure Connect Plus en las conexiones con los recursos de trabajo.....39
Pasos para activar BlackBerry Secure Connect Plus..... 40
Requisitos del servidor y del dispositivo..... 40
Equilibrio de carga y alta disponibilidad de BlackBerry Secure Connect Plus..... 42
BlackBerry Secure Connect Plus y BlackBerry Connectivity Node.....42
Activación y configuración de la conectividad de la empresa y BlackBerry Secure Connect Plus.....42
Resolución de problemas de BlackBerry Secure Connect Plus..... 46
Configuración de conexiones de red para aplicaciones de BlackBerry Dynamics.....49
Creación de un perfil de conectividad de BlackBerry Dynamics.....50
Enrutamiento de todos los datos de aplicaciones de BlackBerry Dynamics a través de BlackBerry Proxy..... 50
Adición de un servidor de aplicaciones a un perfil de conectividad de BlackBerry Dynamics..... 51
Uso de BlackBerry 2FA para establecer conexiones seguras a los recursos cruciales.....51
Configuración de la autenticación de registro único de los dispositivos..... 52
Requisitos previos: uso de la autenticación de Kerberos para los dispositivos..... 52
Autenticación basada en certificados de iOS 8 y posteriores..... 53
Creación de un perfil de registro único..... 53
Filtrado de contenido web en los dispositivos iOS 55
Creación de un perfil de filtro de contenido web.....56
Gestión del correo y de los dominios web para los dispositivos iOS.....57
Creación de un perfil de dominios gestionados..... 57

Creación de un perfil de AirPrint ... 58
Configuración de perfiles de AirPlay para los dispositivos iOS ... 59
Creación de un perfil de AirPlay ... 59
Control del uso de la red de las aplicaciones de trabajo en los dispositivos iOS ... 60
Creación de un perfil de uso de red ... 60

Correo, calendario y contactos ... 61
Configuración del correo de trabajo para dispositivos ... 61
Crear un perfil de correo electrónico ... 61
Creación de un perfil de correo IMAP/POP3 ... 63
Protección de datos de correo electrónico mediante BlackBerry Secure Gateway ... 64
Ampliación de la seguridad del correo mediante S/MIME ... 64
Ampliación de la seguridad del correo mediante PGP ... 68
Aplicación de un correo protegido mediante la clasificación de mensajes ... 69
Configuración de dominios permitidos y restringidos en dispositivos con un espacio de trabajo ... 70
Uso de Enlace de Exchange ... 70
Permitir que un dispositivo tenga acceso a Microsoft ActiveSync ... 71
Bloqueo de un dispositivo para que no acceda a Microsoft ActiveSync ... 71
Comprobación para permitir que un dispositivo tenga acceso al correo de trabajo y a los datos del organizador ... 71
Creación de un perfil de enlace ... 72
Configuración de los perfiles de CardDAV y CalDAV para los dispositivos iOSy macOS ... 72
Creación de un perfil CardDAV ... 72
Creación de un perfil CalDAV ... 73

Certificados ... 74
Pasos para utilizar certificados con dispositivos ... 74
Integración de BlackBerry UEM con el software PKI de la empresa ... 74
Conectar BlackBerry UEM al software de Entrust de la empresa ... 75
Conectar BlackBerry UEM al servidor de Entrust IdentityGuard de su empresa para utilizar credenciales inteligentes ... 75
Conectar BlackBerry UEM al software de OpenTrust de la empresa ... 76
Conexión de BlackBerry UEM al conector de PKI de BlackBerry Dynamics de la empresa ... 76
Conexión de BlackBerry UEM a la solución PKI basada en aplicación de su empresa ... 77
Integración de certificados de cliente en los dispositivos ... 77
Envío de certificados a dispositivos mediante perfiles ... 79
Elección de perfiles para enviar certificados de cliente a los dispositivos ... 80
Envío de certificados de CA a los dispositivos ... 81
Uso de perfiles de credenciales de usuario para enviar certificados a los dispositivos ... 82
Uso de SCEP para enviar certificados de cliente a los dispositivos ... 90
Envío del mismo certificado de cliente a varios dispositivos ... 91
Especificar el certificado utilizado por una aplicación ... 92

Políticas, estándares y conformidad de dispositivos ... 93
Pasos para configurar las políticas y los estándares de la empresa para dispositivos ... 93
Gestión de dispositivos con políticas de TI ... 93
Restricción o autorización de las capacidades del dispositivo ... 94
Establecimiento de los requisitos de la contraseña del dispositivo ... 94
¿Cómo elige BlackBerry UEM qué política de TI asignar? ... 107
Creación y gestión de políticas de TI ... 107

Control de las capacidades del dispositivo con BlackBerry OS mediante políticas de TI..... 111
Control de BlackBerry Dynamics en dispositivos de usuarios..... 111
Creación de un perfil de BlackBerry Dynamics..... 111
Cumplimiento de las reglas de los dispositivos..... 112
Creación de un perfil de cumplimiento..... 112
Cree una plantilla para las notificaciones de conformidad por correo electrónico..... 113
Gestión de perfiles de conformidad de BlackBerry Dynamics..... 114
Configuración de Enterprise Management Agent..... 115
Creación de un perfil de Enterprise Management Agent..... 115
Limitación de los dispositivos a una única aplicación..... 115
Crear un perfil de modo de bloqueo de la aplicación..... 116
Control de las versiones de software instaladas en los dispositivos..... 117
Crear un perfil de requisitos de solicitud de servicio del dispositivo para dispositivos Android con activaciones Solo espacio de trabajo..... 118
Crear un perfil de requisitos de solicitud de servicio del dispositivo para dispositivos con Samsung KNOX..... 118
Crear un perfil de requisitos de solicitud de servicio del dispositivo para dispositivos con BlackBerry 10..... 119
Presentación de los usuarios que están ejecutando una versión de software rechazada..... 120
Presentación de la información de la empresa en los dispositivos..... 120
Crear avisos de la empresa..... 121
Creación de un perfil de dispositivo..... 122
Uso de servicios de ubicación en los dispositivos..... 123
Configurar las opciones del servicio de ubicación..... 123
Creación de un perfil de servicio de ubicación..... 124
Desactivación de las notificaciones fuera de las horas laborables..... 125
Crear un perfil de no molestar..... 125
Administración de las características de iOS mediante perfiles de carga personalizados..... 126
Creación de un perfil de carga personalizado..... 126
Configurar el diseño de las aplicaciones en dispositivos iOS supervisados..... 127
Configuración de Windows Information Protection para dispositivos con Windows 10..... 128
Creación de un perfil de Windows Information Protection..... 128

Aplicaciones..... 129

Adición de aplicaciones a la lista de aplicaciones..... 129
Adición de aplicaciones públicas a la lista de aplicaciones..... 129
Adición de aplicaciones internas a la lista de aplicaciones..... 138
Adición o cambio de la configuración de la aplicación..... 144
Agregar accesos directos de aplicación..... 145
Cómo impedir que los usuarios instalen aplicaciones específicas..... 146
Pasos para impedir que los usuarios instalen aplicaciones específicas..... 147
Agregue una aplicación a la lista de aplicaciones restringidas..... 147
Gestión de aplicaciones en la lista de aplicaciones..... 148
Eliminación de una aplicación de la lista de aplicaciones..... 149
Cambio de si una aplicación es obligatoria u opcional..... 149
Notificaciones del dispositivo para aplicaciones nuevas y actualizadas..... 149
Comportamiento de la aplicación en los dispositivos iOS..... 150
Comportamiento de la aplicación en los dispositivos Android..... 154
Comportamiento de la aplicación en los dispositivos Samsung KNOX..... 156
Comportamiento de las aplicaciones en dispositivos Android que utilizan un perfil de trabajo..... 164
Comportamiento de la aplicación en los dispositivos BlackBerry..... 165
Comportamiento de la aplicación en los dispositivos Windows 10..... 166

Administración de grupos de aplicaciones ... 167
Presentación del estado de las aplicaciones y los grupos de aplicaciones asignados a las cuentas de usuario ... 169
Presentación de las aplicaciones que están asignadas a grupos de usuarios ... 169
Presentación y personalización de la lista de aplicaciones ... 169
Actualización de la lista de aplicaciones ... 170
Actualizar permisos de aplicaciones para aplicaciones con perfiles de trabajo de Android ... 170
Aceptar permisos de aplicaciones para aplicaciones con perfiles de trabajo de Android ... 171
Gestión de aplicaciones de BlackBerry Dynamics ... 172
Gestión de la configuración de una aplicación de BlackBerry Dynamics ... 172
Gestión de servicios de aplicaciones de BlackBerry Dynamics ... 177
Configuración de Kerberos para aplicaciones de BlackBerry Dynamics ... 179
Adición del catálogo de aplicaciones de trabajo a BlackBerry Dynamics Launcher ... 180
Generación de claves de acceso para aplicaciones de BlackBerry Dynamics ... 181
Enviar una clave de desbloque de aplicaciones de BlackBerry Dynamics a un usuario ... 182
Gestión de aplicaciones protegida por Microsoft Intune ... 182
Creación de un perfil de protección de aplicación de Microsoft Intune ... 182
Borrar aplicaciones gestionadas por Microsoft Intune ... 183
Gestión de las cuentas de VPP de Apple ... 183
Adición de una cuenta de VPP de Apple ... 183
Edición de una cuenta de VPP de Apple ... 184
Actualización de la información de la cuenta de VPP de Apple ... 184
Eliminación de una cuenta de VPP de Apple ... 184
Asignación de licencias VPP de Apple a los dispositivos ... 185
Clasificar la instalación de aplicaciones ... 186
Editar la lista de clasificación de instalación de aplicaciones ... 186
Eliminar una aplicación de la lista de clasificación de instalación de aplicaciones ... 186
Visualización de las listas de aplicaciones personales ... 186
Visualización de la lista de aplicaciones personales en la consola de gestión ... 187
Desactivación de la recopilación de aplicaciones personales ... 187
Valoración y comentarios relativos a aplicaciones ... 188
Activar o desactivar las valoraciones y los comentarios para todas las aplicaciones ... 188
Activación de la opción de valoración y comentarios para aplicaciones existentes ... 189
Visualización de comentarios de aplicaciones en la consola de gestión ... 189
Especificación de la configuración de valoración y comentarios para varias aplicaciones ... 189
Eliminar clasificaciones y comentarios sobre la aplicación ... 190
Gestión del icono Work Apps para los dispositivos iOS ... 190
Personalización del icono Aplicaciones de trabajo ... 190
Desactivación de la aplicación Work Apps para iOS ... 191
Gestión de notificaciones para aplicaciones en dispositivos iOS supervisados ... 191
Crear perfil de notificación por aplicación ... 191
Establezca el nombre de la empresa para BlackBerry World ... 192
Administración de aplicaciones en dispositivos con BlackBerry OS ... 193
Preparar la distribución de aplicaciones BlackBerry Java Applications ... 193
Configuración de las políticas de control de aplicaciones ... 194
Políticas de control de aplicaciones para las aplicaciones que no figuran en la lista ... 197
Creación de configuraciones de software ... 198
Instalación de aplicaciones BlackBerry Java Applications en un dispositivo con BlackBerry OS en un equipo central ... 200
Presentación de los usuarios que tienen una aplicación BlackBerry Java Application instalada en sus dispositivos con BlackBerry OS ... 201
Reglas de reconciliación para conflictos de ajustes en las configuraciones de software ... 201

Usuarios y grupos..... 208
Pasos para crear grupos y cuentas de usuario..... 208
Creación de funciones de usuario..... 208
Capacidades de BlackBerry UEM Self-Service..... 208
Cree una función de usuario..... 209
Cómo elige BlackBerry UEM qué función de usuario asignar..... 210
Clasifique las funciones de usuario..... 210
Asigne una función de usuario a un grupo..... 210
Asigne una función de usuario a un usuario..... 210
Creación y administración de cuentas de usuario..... 211
Creación de una cuenta de usuario..... 211
Creación de cuentas de usuario desde un archivo .csv..... 213
Consulta de una cuenta de usuario..... 216
Adición de notas a una cuenta de usuario..... 217
Gestione varias cuentas de usuario al mismo tiempo..... 217
Envío de un correo a los usuarios..... 217
Enviar una contraseña de BlackBerry UEM Self-Service a varios usuarios..... 218
Edición de la información de la cuenta de usuario..... 218
Sincronización de la información del usuario del directorio..... 219
Elimine los servicios de un usuario..... 219
Active los servicios de un usuario..... 220
Eliminar una cuenta de usuario..... 221
Agregar usuarios a los grupos de usuarios..... 221
Eliminación de un usuario de un grupo de usuarios..... 222
Cambio de los grupos de usuarios a los que pertenece un usuario..... 222
Asignar un perfil o una política de TI a una cuenta de usuario..... 222
Adición de un certificado de cliente a una cuenta de usuario..... 223
Cambie un certificado de cliente por una cuenta de usuario..... 224
Renovación o eliminación de un certificado de BlackBerry Dynamics para una cuenta de usuario...224
Adición de un certificado de cliente a un perfil de credenciales de usuario..... 224
Cambie un certificado de cliente por un perfil de credenciales de usuario..... 225
Asignación de una aplicación a una cuenta de usuario..... 225
Asignación de un grupo de aplicaciones a una cuenta de usuario..... 227
Asignación de una política de TI de BlackBerry OS, un perfil o una configuración de software a una cuenta de usuario..... 228
Presentación de las reglas de políticas de TI de BlackBerry OS resueltas que se asignan a una cuenta de usuario..... 229
Creación y administración de grupos de usuarios..... 230
Creación de grupos vinculados a directorios..... 230
Creación de un grupo local..... 232
Consulta de un grupo de usuarios..... 233
Cambio del nombre de un grupo de usuarios..... 233
Eliminar un grupo de usuarios..... 233
Adición de grupos anidados a un grupo de usuarios..... 233
Eliminación de grupos anidados de un grupo de usuarios..... 234
Asignación de un perfil o una política de TI a un grupo de usuarios..... 234
Asignación de una aplicación a un grupo de usuarios..... 234
Asignación de un grupo de aplicaciones a un grupo de usuarios..... 236
Asignación de una política de TI de BlackBerry OS, un perfil o una configuración de software a un grupo de usuarios..... 238
Creación y gestión de grupos de dispositivos compartidos..... 239

Crear un grupo de dispositivos compartidos....239
Activar un dispositivo compartido....239
Ver el historial de desinscripciones de un usuario....240
Editar la suscripción de usuarios para un grupo de dispositivos compartidos....240
Eliminar un dispositivo del grupo de dispositivos compartidos....240
Eliminar un grupo de dispositivos compartidos....241
Asignar una aplicación a un grupo de dispositivos compartidos....241
Asignar una política de TI o un perfil a un grupo de dispositivos compartidos....242
Creación de grupos de dispositivos....242
Creación de un grupo de dispositivos....243
Edite un grupo de dispositivos....244
Definición de parámetros de grupos de dispositivos....244
Presentación de un grupo de dispositivos....245
Cambie el nombre de un grupo de dispositivos....246
Eliminar un grupo de dispositivos....246
Presentación y personalización de la lista de usuarios....246
Establezca la vista predeterminada o avanzada....246
Seleccione la información que desea que aparezca en la lista de usuarios....247
Filtrado de la lista de usuarios....247
Clasificación de la lista de usuarios....247
Exportación de la lista de usuarios a un archivo .csv....248
Cambio de la etiqueta de la propiedad de dispositivo....248

Activación del dispositivo....249
Pasos para activar los dispositivos....249
Requisitos: activación....249
Gestión de las contraseñas de activación....250
Especificación de la configuración predeterminada para las contraseñas de activación....251
Permitir que los usuarios activen varios dispositivos con diferentes tipos de activación....252
Hacer caducar manualmente una contraseña de activación....252
Establezca una contraseña de activación y envíe un mensaje de correo de activación....252
Envío de un mensaje de correo electrónico de activación a varios usuarios....253
Autorización a usuarios para configurar contraseñas de activación en BlackBerry UEM Self-Service....254
Activación del registro de usuario con BlackBerry Infrastructure....254
Habilitar la notificación al usuario cuando se ha activado un dispositivo....255
Soporte de activaciones para dispositivos Android con un perfil de trabajo....255
Es compatible con las activaciones de perfiles de trabajo de Android con un dominio G Suite....255
Es compatible con las activaciones de perfiles de trabajo de Android con un dominio Google Cloud....256
Activación de un BlackBerry Hub unificado....256
Compatibilidad con las activaciones de Windows 10....257
Creación de perfiles de activación....257
Creación de un perfil de activación....257
Tipos de activación: dispositivos con BlackBerry 10....259
Tipos de activación: dispositivos iOS....260
Tipos de activación: dispositivos macOS....261
Tipos de activación: dispositivos Android....261
Tipos de activación: dispositivos Windows....267
Activación detallada para usuarios....267
Activación de dispositivos Android....267
Activar un dispositivo iOS....270

Activar un dispositivo BlackBerry 10 ... 271
Activar un dispositivo Windows Phone ... 271
Activar un dispositivo Windows 10 Mobile ... 272
Activar un dispositivo macOS ... 273
Activar un dispositivo Apple TV ... 274
Active una tableta o un equipo Windows 10 ... 274
Activación de un dispositivo mediante QR Code ... 275
Activación de un dispositivo BlackBerry OS ... 276
Active varios dispositivos mediante KNOX Mobile Enrollment ... 276
Activar varios dispositivos mediante inscripción desatendida para dispositivos Android ... 276
Activación de los dispositivos iOS que están inscritos en DEP ... 277
Pasos para activar los dispositivos que están inscritos en DEP ... 277
Registro de dispositivos iOS en DEP y su asignación a un servidor BlackBerry UEM ... 278
Asignación de una configuración de inscripción a dispositivos iOS ... 279
Adición de una configuración de inscripción ... 279
Eliminación de una configuración de inscripción que se ha asignado a los dispositivos iOS ... 280
Eliminación de una configuración de inscripción ... 281
Cambio de los ajustes en una configuración de inscripción ... 281
Presentación de los ajustes de una configuración de inscripción que está asignada a un dispositivo ... 281
Presentación de los datos de usuario para un dispositivo activado ... 281
Activación de dispositivos iOS mediante Apple Configurator 2 ... 281
Pasos para activar los dispositivos con Apple Configurator 2 ... 282
Adición de información del servidor de BlackBerry UEM a Apple Configurator 2 ... 282
Preparación de dispositivos iOS con Apple Configurator 2 ... 282
Bloqueo de activación en los dispositivos iOS ... 283
Activar bloqueo de activación ... 283
Desactive bloqueo de activación ... 284
Visualice el código de desvío del bloqueo de activación ... 284
Activación de dispositivos BlackBerry 10 mediante BlackBerry Wired Activation Tool ... 284
Configuración de BlackBerry Wired Activation Tool e inicio de sesión en una instancia de BlackBerry UEM ... 285
Active los dispositivos BlackBerry 10 mediante BlackBerry Wired Activation Tool ... 285
Sugerencias para la resolución de problemas de la activación del dispositivo ... 286
No se puede completar la activación del dispositivo porque el servidor no tiene más licencias. Para obtener ayuda, contacte con el administrador ... 287
Compruebe el nombre de usuario y la contraseña e inténtelo de nuevo ... 288
Error de instalación del perfil. No se ha podido importar el certificado "AutoMDMCert.pfx" ... 288
Error 3007: el servidor no está disponible ... 288
No se puede contactar con el servidor, compruebe la conectividad o la dirección del servidor ... 288
iOS or macOS device activations fail with an invalid APNs certificate ... 289
Los usuarios no reciben el correo de activación ... 289

Comandos y controles del dispositivo ... 290
Envío de comandos para los usuarios y dispositivos ... 290
Enviar un comando a un dispositivo ... 290
Envío de un comando masivo ... 290
Establecer un tiempo de caducidad para comandos ... 292
Referencia de comandos ... 292
Desactivación de dispositivos ... 302
Ubicar un dispositivo ... 302
Uso del modo perdido para dispositivos iOS supervisados ... 303

Vea las actualizaciones disponibles para dispositivos iOS....303
Restricción de los dispositivos iOS sin supervisión....304
Actualización del SO en dispositivos de iOS supervisados....304
Creación de mensajes de ayuda del dispositivo....305
Crear mensajes de ayuda del dispositivo....305
Permiso para que los usuarios de BlackBerry 10 realicen copias de seguridad de los datos del dispositivo....305
Generación de claves de cifrado....306
Exportación de claves de cifrado....306
Importación de claves de cifrado....306
Eliminación de claves de cifrado....307

Mantenimiento, supervisión y creación de informes....308

Uso de archivos de registro....308
Administración de archivos de registro BlackBerry UEM....308
Cambiar el nivel de registro a Advertir para clientes Microsoft Intune....311
Búsqueda de archivos de registro....311
Lectura de los archivos de registro....312
La auditoría de la actividad de aplicación en BlackBerry 10 y BlackBerry OS dispositivos....318
Presentación de las acciones de dispositivo....319
Recuperación de registros del dispositivo....320
Auditoría de eventos en BlackBerry UEM....322
Configuración de las opciones de auditoría....322
Visualice y filtre los eventos de auditoría de administrador....324
Exportación de eventos de auditoría de administrador a un archivo .csv....324
Exportación de eventos de auditoría de seguridad a un archivo .csv....324
Eliminación de los registros de auditoría....324
Crear notificaciones de eventos....324
Crear una notificación de evento....325
Crear una programación para una notificación de evento....326
Crear una lista de distribución para una notificación de evento....326
Desactivar una notificación de evento....326
Tipos de evento....326
Gestión de trabajos de BlackBerry Dynamics....328
Uso de SNMP para controlar BlackBerry UEM....329
Uso de los informes de panel....329
Cambio del tipo de gráfico....330
Exportación de un informe de panel a un archivo .csv....330
Visualización de actividad de llamadas telefónicas y SMS/MMS para dispositivos Android con un perfil de trabajo y dispositivos Samsung KNOX Workspace....330
Ver y guardar un informe de dispositivo....331
Exportación de informes de implementación de aplicaciones....331
Exportación de un informe de implementación de aplicaciones a un archivo .html....331
Informes de infracción de conformidad y actividad de aplicaciones de BlackBerry Dynamics....332
Exportación de informes de aplicaciones de BlackBerry Dynamics a un archivo .csv....332
Control del rendimiento de la aplicación BlackBerry Work....332
Activar control de BlackBerry Work....332
Ver notificaciones de alerta de rendimiento del dispositivo....332
Ver una alerta de rendimiento para un único dispositivo....333

Configuraciones de perfil....334

Configuración del perfil de correo....334
Común: ajustes del perfil de correo....334
BlackBerry 10: ajustes del perfil de correo....335
iOS: ajustes del perfil de correo....344
macOS: ajustes del perfil de correo....349
Android: ajustes del perfil de correo....350
Windows: ajustes del perfil de correo....357
Configuración del perfil de correo IMAP/POP3....358
Común: configuración del perfil de correo IMAP/POP3....359
iOS y macOS: configuración del perfil de correo IMAP/POP3....360
Android: configuración del perfil de correo IMAP/POP3....363
Windows: configuración del perfil de correo IMAP/POP3....363
Ajustes del perfil de Wi-Fi....364
Común: ajustes del perfil Wi-Fi....365
BlackBerry 10: ajustes del perfil de Wi-Fi....365
iOS y macOS: configuración de perfil Wi-Fi....370
Android: ajustes del perfil de Wi-Fi....377
Windows: ajustes del perfil de Wi-Fi....381
Configuración de perfil VPN....386
BlackBerry 10: ajustes del perfil de VPN....387
iOS y macOS: configuración del perfil de VPN....403
Android: ajustes del perfil de VPN....413
Windows 10: ajustes del perfil de VPN....419
Ajustes del perfil SCEP....426
Común: ajustes del perfil SCEP....426
BlackBerry 10: ajustes del perfil SCEP....428
iOS: ajustes del perfil SCEP....432
macOS: ajustes del perfil de SCEP....434
Android: ajustes del perfil SCEP....435
Windows 10: ajustes del perfil SCEP....438
BlackBerry Dynamics: SCEP profile settings....441
Configuración del perfil de conformidad....444
Común: configuración del perfil de conformidad....444
BlackBerry 10: configuración del perfil de conformidad....447
iOS: configuración del perfil de conformidad....448
macOS: configuración del perfil de conformidad....452
Android: configuración del perfil de conformidad....453
Windows: configuración del perfil de conformidad....456
Ajustes del perfil de BlackBerry Dynamics....459
Configuración del perfil de conectividad de BlackBerry Dynamics....465
Configuración del perfil de conectividad de empresa....467
Común: configuración del perfil de conectividad de empresa....467
BlackBerry 10: configuración del perfil de conectividad de empresa....467
iOS: configuración del perfil de conectividad de empresa....467
Android: configuración del perfil de conectividad de empresa....468
Ajustes del perfil de Enterprise Management Agent....470
BlackBerry 10: ajustes del perfil de Enterprise Management Agent....470
iOS: ajustes del perfil de Enterprise Management Agent....472
Android: ajustes del perfil de Enterprise Management Agent....472
Windows: ajustes del perfil de Enterprise Management Agent....473
Configuración del perfil de Windows Information Protection....474
Windows 10: configuración de perfil de Windows Information Protection....474
Configuración del perfil de protección de aplicaciones de Microsoft Intune....479
Común: configuración del perfil de protección de aplicaciones de Microsoft Intune....479

iOS: configuración del perfil de protección de aplicaciones de Microsoft Intune.....482
Android: configuración del perfil de protección de aplicaciones de Microsoft Intune..... 483

Hoja de cálculo de referencia de políticas.....486

Glosario.....487

Aviso legal..... 491

Pasos para comenzar a utilizar BlackBerry UEM

Paso	Acción
1	Planifique la instalación de BlackBerry UEM.
2	Instale BlackBerry UEM o actualice a la última versión de BlackBerry UEM.
3	Si utiliza BlackBerry Work o BlackBerry Connect, instale o actualice y configure BlackBerry Enterprise Mobility Server.
4	Iniciar sesión en BlackBerry UEM.
5	Configure BlackBerry UEM en función de los requisitos de su empresa.
6	Si desea compartir el trabajo de administración con otro personal de TI, cree administradores.
7	Configure las conexiones de trabajo. Por ejemplo, correo, Wi-Fi y VPN.
8	Establezca las reglas para gestionar la seguridad y el comportamiento de los dispositivos mediante políticas de TI.
9	Configure los estándares de dispositivo. Por ejemplo, reglas de cumplimiento.
10	Si su empresa utiliza BlackBerry Dynamics, configure los ajustes de BlackBerry Dynamics.
11	Determine las aplicaciones que se enviarán a los dispositivos y agréguelas a BlackBerry UEM.
12	Controle el modo en que los dispositivos se activan y se gestionan en BlackBerry UEM mediante perfiles de activación.
13	Cree los grupos de usuarios o cuentas de usuario que sean necesarios.
14	Asigne perfiles y políticas de TI a grupos de usuarios o cuentas de usuario.

Paso	Acción
15	Asigne aplicaciones a grupos de usuarios o cuentas de usuario.
16	Pida a los usuarios que activen los dispositivos en BlackBerry UEM.

Características compatibles por tipo de dispositivo

Esta referencia rápida compara las capacidades compatibles de los dispositivos con BlackBerry 10, BlackBerry OS (versión 5.0 a 7.1), iOS, macOS, Android y Windows en la versión 12.7 de BlackBerry UEM.

La compatibilidad con los dispositivos BlackBerry OS requiere una actualización de BES5 a BlackBerry UEM.

Para obtener más información acerca de las versiones OS compatibles, consulte la Matriz de compatibilidad.

Características del dispositivo

Función	BlackBerry 10	BlackBerry OS	iOS	macOS	Android	Windows
Activación inalámbrica	√	√	√	√	√	√
Activación inalámbrica mediante un código QR			√		√	
Activación con cable mediante BlackBerry Wired Activation Tool	√					
Aplicación de cliente necesaria para la activación			√ [1]		√	√ [2]
Personalización del acuerdo de los términos de uso para la activación	√		√	√	√	√ [3]
Restricción de la activación por modelo de dispositivo	√		√	√	√	√ [4]

Función	BlackBerry 10	BlackBerry OS	iOS	macOS	Android	Windows
Presentación y exportación del informe del dispositivo (por ejemplo, detalles de hardware)	√	√	√	√	√	√
Restringir los dispositivos sin supervisión			√[5]	√[5]		

[1] Para dispositivos iOS inscritos en DEP, la aplicación cliente debe estar asignada a los usuarios o grupos.

[2] Para los dispositivos Windows Phone 8.x únicamente.

[3] Para los dispositivos Windows 10 únicamente.

[4] Para los dispositivos Windows Phone 8.x y Windows 10 Mobile únicamente.

[5] Para los dispositivos activados con controles MDM o Privacidad del usuario con licencias basadas en SIM únicamente.

Características de seguridad

Función	BlackBerry 10	BlackBerry OS	iOS	macOS	Android	Windows
Separación de los datos personales y de trabajo	√	√	√[1]		√[2]	√[4]
Privacidad del usuario para los datos personales	√	√	√[1]		√[2]	
Cifrado de los datos de trabajo almacenados	√	√	√[1]		√[2]	√[4]
Protección de los dispositivos mediante el envío de comandos de TI	√	√	√	√	√	√
Control de las capacidades del dispositivo mediante políticas de TI	√	√	√	√	√	√

Función	BlackBerry 10	BlackBerry OS	iOS	macOS	Android	Windows
Eliminación de los datos de trabajo tras un periodo de inactividad	√		√ [1]		√ [1]	
Aplicar los requisitos de la contraseña	√	√	√	√	√	√
Aplicar el cifrado de la tarjeta de memoria	√	√			√ [3]	
Aplicar el cifrado del almacenamiento interno	√	√			√	√

[1] Requiere las aplicaciones de BlackBerry Dynamics.

[2] Requiere Samsung KNOX Workspace, perfiles de trabajo de Android o aplicaciones de BlackBerry Dynamics.

[3] Para los dispositivos Samsung KNOX únicamente.

[4] Para los dispositivos Windows 10 únicamente.

Envío de certificados a los dispositivos

Función	BlackBerry 10	BlackBerry OS	iOS	macOS	Android	Windows
Perfiles de certificado de CA	√		√	√	√	√
Perfiles SCEP	√		√	√	√	√ [1]
Perfiles de certificado compartido			√	√	√	
Perfiles de credenciales de usuario	√		√	√	√	

[1] Para los dispositivos Windows 10 únicamente.

Administración de las conexiones de trabajo de los dispositivos

Función	BlackBerry 10	BlackBerry OS	iOS	macOS	Android	Windows
Perfiles de BlackBerry 2FA	√		√		√	
Perfiles de conectividad de BlackBerry Dynamics			√	√	√	√
Perfiles de CalDAV			√	√		
Perfiles de CardDAV			√	√		
Perfiles de recuperación de certificados	√					
Conectividad de la empresa	√					
BlackBerry Secure Connect Plus	√		√ [1]		√ [2]	
Perfiles de correo de Exchange ActiveSync	√		√	√	√ [3]	√
BlackBerry Secure Gateway			√			
Perfiles de correo IMAP/POP3			√	√	√	√
Perfiles de proxy	√		√	√	√	√ [4]
Perfiles de registro único	√		√			
Perfiles VPN	√	√	√	√	√ [5]	√ [6]
Perfiles de Wi-Fi	√	√	√	√	√	√
Otros perfiles específicos de SO	• Perfiles CRL • Perfiles OCSP				• Perfiles CRL [7]	• Perfiles de Windows Information Protection [7]

[1] Solo para dispositivos que ejecutan iOS 9.0 y posteriores.

[2] Solo para dispositivos Android que tienen un perfil de trabajo y dispositivos KNOX Workspace.

[3] Solo para dispositivos Motorola que son compatibles con EDM API, dispositivos con Android que tienen un perfil de trabajo y dispositivos KNOX.

[4] Únicamente para dispositivos Windows 10 (configure las opciones del servidor proxy en los perfiles VPN) y dispositivos Windows 10 Mobile (configure las opciones del servidor proxy en los perfiles de Wi-Fi).

[5] Para los dispositivos KNOX Workspace únicamente.

[6] Para los dispositivos Windows 10 únicamente.

[7] Solo para dispositivos BlackBerry con Android y tecnología Android 7.0 y posteriores.

Gestión de los estándares de la empresa para dispositivos

Función	BlackBerry 10	BlackBerry OS	iOS	macOS	Android	Windows
Perfiles de activación	√		√	√	√	√
Perfiles de modo de bloqueo de la aplicación			√ [1]		√ [1]	√ [1]
Perfiles de BlackBerry Dynamics			√	√	√	√
Perfiles de conformidad de BlackBerry Dynamics [2]			√	√	√	√
Perfiles de conformidad	√		√		√	√ [3]
Perfiles de dispositivo	√		√		√	√ [4]
Perfiles de Enterprise Management Agent	√		√		√	√
Perfiles de servicio de ubicación			√		√	√ [5]

Función	BlackBerry 10	BlackBerry OS	iOS	macOS	Android	Windows
Otros perfiles específicos de SO	• Perfiles de requisitos de versión de software del dispositivo	• Reglas de control de acceso • Configuración de software	• Perfiles de AirPlay • Perfiles de AirPrint • Perfiles de carga personalizados • Perfiles de dominios gestionados • Perfiles de uso de red • Perfiles de notificación por aplicación [6] • Perfiles de filtro de contenido web			

[1] Solo para dispositivos iOS supervisados, dispositivos KNOX que se han activado con Controles de MDM y dispositivos Windows 10 Education y Windows 10 Enterprise.

[2] Si su entorno incluye Good Control y BlackBerry UEM, después de actualizar y sincronizar Good Control con BlackBerry UEM, los perfiles de conformidad existentes en Good Control se importan a BlackBerry UEM como perfiles de conformidad de BlackBerry Dynamics que contienen la configuración de conformidad de Good Control.

[3] Para los dispositivos Windows Phone 8.x únicamente.

[4] Para los dispositivos Windows 10 únicamente.

[5] Para los dispositivos Windows 10 Mobile únicamente.

[6] Solo para dispositivos con iOS supervisados que ejecutan iOS 9.3 y posterior.

Protección de dispositivos perdidos o robados

Función	BlackBerry 10	BlackBerry OS	iOS	macOS	Android	Windows
Especificar contraseña de dispositivo	√	√			√	√ [1]

Función	BlackBerry 10	BlackBerry OS	iOS	macOS	Android	Windows
Bloquear dispositivo	√	√	√	√	√	√ [1]
Bloqueo de activación			√ [2]			
Especificar contraseña de espacio de trabajo y bloquear					√ [3]	
Desbloquear dispositivo y borrar contraseña			√		√	
Eliminar todos los datos del dispositivo	√	√	√	√	√ [4]	√
Eliminar solo los datos de trabajo	√	√	√	√	√	√

[1] Para los dispositivos Windows Phone 8.x y Windows 10 Mobile únicamente.

[2] Solo para dispositivos que ejecutan iOS 7.0 y posteriores.

[3] Solo para dispositivos Android que tienen un perfil de trabajo que se ejecuta con Android 7.0 y posteriores.

[4] En los dispositivos Motorola que son compatibles con EDM API, la información sobre la tarjeta de memoria también se ha eliminado. En los dispositivos KNOX Workspace, puede elegir si desea eliminar la información de la tarjeta de memoria.

Configuración de roaming

Función	BlackBerry 10	BlackBerry OS	iOS	macOS	Android	Windows
Desactivación de la sincronización automática cuando se encuentra en roaming	√ [1]		√		√ [2]	

Función	BlackBerry 10	BlackBerry OS	iOS	macOS	Android	Windows
Desactivación de datos cuando se encuentra en roaming	√		√[3]		√ [4]	√

[1] Para la sincronización con el servidor de correo únicamente.

[2] Para los dispositivos KNOX únicamente.

[3] Para los dispositivos con iOS 9.0 o posteriores, puede configurar los ajustes de roaming de datos en un perfil de uso de red.

[4] Solo para dispositivos Android que tienen un perfil de trabajo y dispositivos KNOX.

Gestión de aplicaciones

Función	BlackBerry 10	BlackBerry OS	iOS	macOS	Android	Windows
Distribución de las aplicaciones públicas de la tienda (BlackBerry World, App Store, Google Play, Windows Store)	√		√		√	√
Gestión del catálogo de aplicaciones de trabajo	√	√	√		√	√
Catálogo de aplicaciones de trabajo de marca	√		√			
Gestión de aplicaciones restringidas			√		√ [1]	√ [1]
Distribución de aplicaciones internas	√	√	√		√	√

Función	BlackBerry 10	BlackBerry OS	iOS	macOS	Android	Windows
Añadir accesos directos de aplicación a dispositivos			√	√	√	

[1] No es necesaria una lista de aplicaciones restringidas para los dispositivos Android con perfiles de trabajo, ni para dispositivos KNOX Workspace o Windows 10, ya que solo las aplicaciones que asigna un administrador pueden instalarse en el espacio de trabajo o en dispositivos.

Gestión de aplicaciones de BlackBerry Dynamics en BlackBerry UEM

Las aplicaciones de productividad de BlackBerry Dynamics proporcionan a los usuarios acceso a los datos de trabajo y herramientas de productividad. Las aplicaciones de BlackBerry Dynamics desarrolladas por BlackBerry incluyen las siguientes aplicaciones:

Aplicación	Descripción
BlackBerry Work	La aplicación BlackBerry Work proporciona un acceso seguro al correo de trabajo y permite a los usuarios ver y enviar archivos adjuntos, crear notificaciones de contacto personalizadas y administrar sus mensajes.
BlackBerry Access	BlackBerry Access es un navegador seguro que permite a los usuarios tener acceso a las aplicaciones web e intranets del trabajo. BlackBerry Access también le permite habilitar el acceso a los recursos del trabajo o crear e implementar aplicaciones HTML5 complejas, mientras se mantiene un alto nivel de seguridad y cumplimiento.
BlackBerry Connect	BlackBerry Connect permite la comunicación y la colaboración con la mensajería instantánea segura, la búsqueda de directorios de la empresa y la presencia de usuarios en una interfaz fácil de usar en los dispositivos de los usuarios.
BlackBerry Tasks	BlackBerry Tasks permite a los usuarios crear, editar y gestionar tareas que se sincronizan con Microsoft Exchange.
BlackBerry Notes	BlackBerry Notes permite a los usuarios crear, editar y gestionar notas que se sincronizan con Microsoft Exchange en el dispositivo móvil que elijan.
BlackBerry Docs To Go	BlackBerry Docs To Go permite a los usuarios crear, editar y dar formato a documentos de Microsoft Word y hojas de cálculo de Microsoft Excel que están guardadas en la aplicación o se comparten desde otras aplicaciones de BlackBerry Dynamics. Los usuarios también pueden ver, editar y hacer presentaciones de Microsoft PowerPoint desde sus dispositivos.

Para obtener más información sobre la gestión de aplicaciones de BlackBerry Dynamics, consulte Gestión de aplicaciones de BlackBerry Dynamics y los recursos para administradores de cada aplicación.

También puede utilizar aplicaciones de BlackBerry Dynamics desarrolladas por uno de los muchos socios de aplicaciones de terceros de BlackBerry. Para obtener una lista completa de las aplicaciones disponibles a nivel público, visite BlackBerry Marketplace for Enterprise Software.

También puede desarrollar sus propias aplicaciones de BlackBerry Dynamics mediante BlackBerry Dynamics SDK. Para obtener más información, consulte el contenido referente al SDK de BlackBerry Dynamics.

Dispositivos BlackBerry con Android

PRIV, DTEK y KEY son ejemplos de dispositivos BlackBerry con Android. Para gestionar estos dispositivos con BlackBerry UEM, puede seguir las instrucciones para los dispositivos Android.

Los siguientes tipos de activación están disponibles para los dispositivos BlackBerry con Android:

- Trabajo y personal: privacidad de usuario
- Trabajo y personal: privacidad de usuario (Premium)
- Solo espacio de trabajo
- Solo espacio de trabajo (Premium)
- Controles de MDM
- Privacidad del usuario

Le recomendamos que active los dispositivos BlackBerry con Android mediante un tipo de activación "Trabajo y personal" o "Solo espacio de trabajo" para disfrutar de una experiencia óptima.

Opciones de gestión de dispositivos

BlackBerry UEM admite diversas opciones para la administración de dispositivos. Las opciones que elija dependerán de los tipos de dispositivos que administra y los requisitos de seguridad de la empresa.

BlackBerry UEM admite las siguientes opciones de administración:

- Controles de MDM
- Trabajo y personal
- Privacidad del usuario
- Solo espacio de trabajo

Para cada opción de gestión, debe tener las licencias correctas disponibles y el perfil de activación apropiado asignado a los usuarios.

Para obtener más información acerca de los perfiles de activación, consulte Creación de perfiles de activación.

Para obtener más información sobre las licencias de BlackBerry UEM, consulte el contenido de licencias.

Para obtener más información acerca de la seguridad de las distintas opciones de gestión, consulte el contenido referente a Seguridad.

Administración de dispositivos que no sean smartphones, tabletas y portátiles

Con BlackBerry UEM, puede activar y gestionar dispositivos que no sean smartphones, tabletas y portátiles.

BlackBerry UEM también gestiona los siguientes dispositivos:

- Determinados dispositivos accesorios basados en Android
- Dispositivos Apple TV

Gestión de los dispositivos accesorios

Puede activar y gestionar los dispositivos accesorios Android en BlackBerry UEM. Los dispositivos accesorios, como las gafas inteligentes, proporcionan a los usuarios acceso manos libres a información visual como notificaciones, instrucciones paso a paso, imágenes y vídeo y permiten a los usuarios emitir comandos de voz, escanear códigos de barras y utilizar la navegación GPS.

BlackBerry UEM es compatible con los siguientes dispositivos accesorios:

- Vuzix M300 Smart Glasses

Para gestionar los dispositivos accesorios, siga las instrucciones para dispositivos Android. Las siguientes funciones de BlackBerry UEM son compatibles con los dispositivos accesorios:

- Activación del dispositivo mediante un QR Code
- Políticas de TI
- Wi-Fi, VPN, conectividad de empresa, conformidad y perfiles de certificado
- BlackBerry Secure Connect Service
- Comandos del dispositivo
- Administración de aplicaciones
- Grupos de dispositivos
- Servicios de ubicación

Los dispositivos accesorios utilizan el BlackBerry UEM Client para la activación. Puede activar los dispositivos accesorios mediante un código QR en lugar de una contraseña de activación. Para obtener más información, consulte Activación de un dispositivo mediante QR Code.

Gestionar dispositivos Apple TV

Puede activar y gestionar dispositivos Apple TV en BlackBerry UEM. Apple TV es un reproductor multimedia digital que puede recibir datos y transferirlos a un televisor a través de un cable HDMI.

BlackBerry UEM es compatible con las versiones de Apple TV de segunda generación o posteriores.

Para gestionar los dispositivos Apple TV, siga las instrucciones y utilice los ajustes del perfil para los dispositivos iOS. Las siguientes funciones de BlackBerry UEM son compatibles con Apple TV:

- Activación del dispositivo mediante BlackBerry UEM Self-Service
- Tipo de activación de los controles MDM
- Wi-Fi y perfiles de certificado
- Perfiles de modo de bloqueo de la aplicación
- Comandos del dispositivo

Para evitar que los usuarios activen dispositivos Apple TV, establezca la restricción de modelo de dispositivo en el perfil de activación para no permitir dispositivos Apple TV.

Para activar los dispositivos Apple TV, debe utilizar BlackBerry UEM Self-Service. Para obtener más información, consulte Activar un dispositivo Apple TV.

¿En qué consiste BlackBerry UEM Client ?

BlackBerry UEM Client es una aplicación que permite a los usuarios activar dispositivos en BlackBerry UEM. Se requiere UEM Client para activar los siguientes dispositivos:

- iOS
- Android, incluidos los accesorios de Android wearable devices
- Windows Phone 8

Los usuarios pueden descargar UEM Client de App Store, Google Play, o Windows Store.

La siguiente tabla resume las funciones de UEM Client:

Función de BlackBerry UEM Client	Descripción
Comunicación con BlackBerry UEM	UEM Client permite que BlackBerry UEM se comunique con dispositivos para la activación y la gestión de dispositivos. Para obtener más información sobre los flujos de datos, consulte el contenido de Arquitectura.
Activación	Los usuarios deben descargar la última versión de UEM Client de la tienda de aplicaciones correspondiente y utilizar su dirección de correo y contraseña de activación o QR Code para activar los dispositivos en BlackBerry UEM. En los siguientes casos, los usuarios no tienen que utilizar UEM Client para activar dispositivos: • Para dispositivos iOS, si se utiliza Apple Configurator 2 o el programa de inscripción de dispositivos de Apple, los usuarios no necesitan UEM Client para activar los dispositivos. Los usuarios deben instalar e iniciar la aplicación UEM Client después de la activación si desean aplicar reglas de cumplimiento. • Para dispositivos iOS y Android que no necesitan MDM, los usuarios pueden activar las aplicaciones de BlackBerry Dynamics con las claves de acceso en lugar de utilizar UEM Client.Sin embargo, el uso de UEM Client proporciona beneficios adicionales, como una experiencia de activación coherente que no requiere claves de acceso, el acceso al catálogo de aplicaciones de trabajo en UEM Client o BlackBerry Dynamics Launcher (si está configurado) y la capacidad para los usuarios de autorizar servicios de ubicación (si está configurada). Para obtener más información, consulte Activación del dispositivo.
Desactivación	Los usuarios pueden hacer clic en "Desactivar mi dispositivo" en la sección "Acerca de" de UEM Client para eliminar el dispositivo de BlackBerry UEM y eliminar todos los datos de trabajo del dispositivo.

Función de BlackBerry UEM Client	Descripción
Aplicaciones de trabajo	UEM Client permite a los usuarios buscar y descargar las aplicaciones asignadas, y si está configurado, los usuarios pueden proporcionar valoraciones y comentarios de las aplicaciones. Para los dispositivos iOS activados con privacidad de usuario, los usuarios pueden acceder al catálogo de aplicaciones de trabajo desde un vínculo en el navegador en UEM Client. Para los dispositivos iOS activados con MDM, se ofrece un icono personalizable para las aplicaciones de trabajo en la pantalla de inicio. Para los dispositivos Android, los usuarios pueden acceder al catálogo de aplicaciones de trabajo en UEM Client. Para dispositivos Windows Phone 8, los usuarios pueden acceder al catálogo de aplicaciones de trabajo en UEM Client. Para obtener más información, consulte Aplicaciones.
Perfiles y políticas.	Los perfiles, políticas y certificados que se asignan a los usuarios se muestran en UEM Client.
Conformidad	En la pantalla de inicio de UEM Client, los usuarios pueden tocar "Conformidad" o "Sin conformidad" para ver un informe de estado de los dispositivos basado en el perfil de conformidad asignado. Para los dispositivos que se activan con Apple Configurator 2 o el programa de inscripción de dispositivos de Apple, los usuarios deben instalar e iniciar BlackBerry UEM Client tras la activación si desean aplicar reglas de cumplimiento. Para obtener más información, consulte Cumplimiento de las reglas de los dispositivos.
BlackBerry 2FA	Si está configurado, los usuarios pueden omitir la autenticación en dos fases requerida por BlackBerry 2FA mediante la autenticación previa en UEM Client. Para obtener más información, consulte el contenido de BlackBerry 2FA.
Servicio de ubicación	Si crea un perfil de servicio de ubicación y lo asigna a cuentas de usuario, se solicitará a los usuarios que permitan que UEM Client acceda a la ubicación del dispositivo.
Archivos de registro del dispositivo	Los usuarios pueden enviar archivos de registro del dispositivo por correo electrónico desde UEM Client. Para obtener más información, consulte Recuperación de registros del dispositivo.

Función de BlackBerry UEM Client	Descripción
Acerca de	En la sección "Acerca de" de UEM Client, los usuarios pueden ver toda la información, o parte de ella, en función del tipo de dispositivo y el tipo de activación: • La versión de UEM Client. • La fecha y la hora en las que se activó el dispositivo. • Información de la empresa que puede configurar en el perfil del dispositivo (por ejemplo, la información de contacto de la empresa). • La URL del servidor de BlackBerry UEM. • Contrato de licencia para el usuario final. • Un botón que permite a los usuarios desactivar su dispositivo.

¿En qué consiste BlackBerry UEM Self-Service ?

BlackBerry UEM Self-Service es una aplicación web que puede poner a disposición de los usuarios para que puedan realizar algunas tareas como la creación de contraseñas de activación, el bloqueo de dispositivos o la eliminación de datos de los dispositivos. Los usuarios no necesitan instalar ningún software en sus equipos para utilizar BlackBerry UEM Self-Service.

Debe proporcionar la información de inicio de sesión de BlackBerry UEM Self-Service a los usuarios. Puede enviar esta información en un mensaje de correo electrónico, o editar la plantilla de correo de activación para incluir la información. Los usuarios necesitan la siguiente información:

- Dirección web: la dirección web para BlackBerry UEM Self-Service aparece en la consola de gestión en Configuración > Autoservicio.
- El nombre de usuario y la contraseña: los usuarios del directorio de la empresa pueden iniciar sesión con los nombres de usuario y las contraseñas de la empresa. Para los usuarios locales, debe crear los nombres de usuario y las contraseñas temporales.
- Nombre de dominio: el nombre de dominio es necesario para los usuarios de Microsoft Active Directory.

También puede crear un aviso de inicio de sesión que los usuarios deben leer y aceptar antes de que puedan iniciar sesión en BlackBerry UEM Self-Service.

Para obtener más información sobre BlackBerry UEM Self-Service, consulte la guía del usuario de BlackBerry UEM Self-Service.

Tareas relacionadas

Creación de un aviso de inicio de sesión para las consolas

Servicios de BlackBerry Enterprise Mobility Suite

Además de las funciones de seguridad y productividad proporcionadas por BlackBerry UEM, BlackBerry ofrece más servicios que pueden agregar valor a su dominio de BlackBerry UEM para ayudarle a satisfacer las necesidades exclusivas de su empresa. Puede agregar los siguientes servicios y gestionarlos a través de la consola de gestión de BlackBerry UEM:

Tipo de servicio	Descripción y nombre del servicio
Servicios empresariales	• BlackBerry Workspaces permite a los usuarios sincronizar, editar y compartir archivos y carpetas, así como acceder a ellos de forma segura, desde tabletas y equipos Windows y Mac OS o en dispositivos Android, iOS y con BlackBerry 10. BlackBerry Workspaces protege los archivos mediante la aplicación de controles de DRM para limitar el acceso, incluso después de que se hayan compartido con alguien ajeno a su empresa. • BlackBerry Enterprise Identity proporciona a los usuarios acceso de inicio de sesión único a proveedores de servicios como BlackBerry Workspaces, Box, Workday, WebEx y Salesforce, entre otros. También puede añadir la compatibilidad para servicios SaaS personalizados. • BlackBerry 2FA protege el acceso a los recursos críticos de su empresa mediante la autenticación de dos factores. BlackBerry 2FA utiliza una contraseña que los usuarios deben introducir y una solicitud de seguridad en sus dispositivos Android, iOS o con BlackBerry 10 cada vez que intentan acceder a los recursos. • BlackBerry UEM Notifications permite a los administradores enviar mensajes a los usuarios a través de SMS, teléfono y correo electrónico directamente desde la consola de UEM. Este complemento simplifica las comunicaciones con los usuarios finales y los grupos de usuarios, ya que evita la necesidad de disponer de soluciones de mensajería adicionales.
Plataforma BlackBerry Dynamics	• BlackBerry Enterprise Mobility Server (BEMS) proporciona servicios adicionales para las aplicaciones de BlackBerry Dynamics. BEMS integra los servicios siguientes: BlackBerry Mail, BlackBerry Connect, BlackBerry Presence y BlackBerry Docs. Cuando estos servicios están integrados, los usuarios pueden comunicarse entre sí mediante mensajería instantánea segura, ver la presencia de usuarios en tiempo real en las aplicaciones de BlackBerry Dynamics y acceder, sincronizar y compartir el servidor de archivos de trabajo y documentos de Microsoft SharePoint. • BlackBerry Dynamics SDK permite a los desarrolladores crear aplicaciones seguras para dispositivos Android y iOS y equipos con Mac OS y Windows. Es el lado del cliente de la plataforma BlackBerry Dynamics.
Aplicaciones de productividad de BlackBerry Dynamics	• BlackBerry Work proporciona todo lo que necesitan los usuarios para mover de forma segura su trabajo, incluido el correo, el calendario y los contactos (sincronización completa con Microsoft Exchange). La aplicación también proporciona colaboración de documentos avanzada. BlackBerry Work separa los datos de trabajo de los datos personales y permite una integración perfecta con otras aplicaciones de trabajo sin la necesidad de perfiles de MDM en el dispositivo. • BlackBerry Access permite a los usuarios acceder de forma segura a la intranet de su empresa con el dispositivo móvil que elijan. • BlackBerry Connect mejora la comunicación y la colaboración con la mensajería instantánea segura, la búsqueda de directorios de la empresa y la presencia de usuarios en una interfaz fácil de usar en el dispositivo del usuario. • BlackBerry Tasks permite a los usuarios crear, editar y gestionar notas que se sincronizan con Microsoft Exchange en sus dispositivos Android e iOS. • BlackBerry Notes permite a los usuarios crear, editar y gestionar notas que se sincronizan con Microsoft Exchange en el dispositivo móvil que elijan.

Para obtener más información acerca de las diferentes licencias de BlackBerry Enterprise Mobility Suite y cómo obtenerlas, consulte el contenido referente a Licencias.

Inicio de sesión en BlackBerry UEM

La consola de gestión le permite realizar tareas administrativas en los dispositivos de la empresa que están administrados por BlackBerry UEM.

Antes de empezar:

- Localice la dirección web (por ejemplo, https://<*nombre del host*>/admin/index.jsp.) y la información de inicio de sesión de la consola de gestión. Puede encontrar dicha información en la bandeja de entrada de la cuenta de correo asociada a su cuenta BlackBerry UEM.
- Debe saber el método de autenticación y el dominio (aplicable a la autenticación de Microsoft Active Directory únicamente).

1. En el navegador, escriba la dirección web de la consola de gestión de BlackBerry UEM de la empresa.
2. En el campo **Nombre de usuario**, escriba su nombre de usuario.
3. En el campo **Contraseña**, escriba su contraseña.
4. Si fuese necesario, en la lista desplegable **Iniciar sesión con**, realice una de las acciones siguientes:
   - Haga clic en **Autenticación directa**.
   - Haga clic en **Autenticación de LDAP**.
   - Haga clic en **Autenticación de Microsoft Active Directory**. En el campo**Dominio**, escriba el dominio de Microsoft Active Directory.
5. Haga clic en **Iniciar sesión**.

Después de terminar: Puede cambiar la contraseña de inicio de sesión con un clic en el icono de usuario de la esquina superior derecha de la consola de gestión.

Wi-Fi, VPN, BlackBerry Secure Connect Plus y otras conexiones de trabajo

Puede utilizar los perfiles para configurar y administrar las conexiones de trabajo para los dispositivos de la empresa. Las conexiones de trabajo definen el modo en que los dispositivos se conectan a los recursos de trabajo en el entorno de la empresa, tales como servidores de correo, servidores proxy, redes Wi-Fi y VPN. Puede especificar la configuración de los dispositivos con BlackBerry 10, iOS, macOS, Android y Windows en el mismo perfil y, a continuación, asignar el perfil a las cuentas de usuarios, a los grupos de usuarios o a los grupos de dispositivos.

Pasos para configurar las conexiones de trabajo para dispositivos

Al configurar las conexiones de trabajo para dispositivos, debe realizar las acciones siguientes:

Paso	Acción
1	Cree perfiles para configurar la forma en que los dispositivos se conectan a los recursos de trabajo. Por ejemplo, crear un perfil de correo, un perfil de Wi-Fi, un perfil de VPN, un perfil de conectividad de empresa y un perfil de conectividad de BlackBerry Dynamics.
2	Si fuera necesario, clasifique los perfiles.
3	Asigne perfiles a las cuentas de usuario, a los grupos de usuarios o a los grupos de dispositivos.

Procedimiento recomendado: creación de perfiles de conexión de trabajo

Algunos perfiles de conexión de trabajo pueden incluir uno o más perfiles asociados. Al especificar un perfil asociado, se vincula un perfil a un perfil de conexión de trabajo y los dispositivos deberán utilizar el perfil asociado al utilizar el perfil de conexión de trabajo.

Considere las siguientes directrices:

- Determine qué conexiones de trabajo se requieren para los dispositivos en la empresa.
- Cree perfiles que se puedan asociar a otros perfiles antes de crear los perfiles de conexión de trabajo que los utilizan.
- Utilice variables cuando proceda.

Puede asociar perfiles de certificado y de proxy a varios perfiles de conexión de trabajo. Debe crear perfiles en el siguiente orden:

1. Perfiles de certificado
2. Perfiles de proxy
3. Perfiles de conexión de trabajo tales como correo, VPN y Wi-Fi

Por ejemplo, si crea un perfil de Wi-Fi en primer lugar, no se puede asociar un perfil de proxy al perfil de Wi-Fi cuando éste se crea. Después de crear un perfil de proxy, debe cambiar el perfil de Wi-Fi para asociarlo al perfil de proxy.

Conceptos relacionados

Envío de certificados a dispositivos mediante perfiles

Referencia relacionada

Uso de variables en perfiles

Configuración de las redes Wi-Fi de trabajo para dispositivos

Puede utilizar un perfil de Wi-Fi para especificar el modo en que los dispositivos se conectan a una red Wi-Fi de trabajo detrás del firewall. Se puede asignar un perfil de Wi-Fi a cuentas de usuarios, a grupos de usuarios y a grupos de dispositivos.

Dispositivo	Aplicaciones y conexiones de red
BlackBerry 10	De forma predeterminada, tanto las aplicaciones de trabajo como las personales pueden utilizar los perfiles Wi-Fi guardados en el dispositivo para conectarse a la red de la empresa. Las aplicaciones de trabajo también pueden utilizar BlackBerry Infrastructure para conectarse a la red de la empresa. Si los estándares de seguridad de la empresa no permiten aplicaciones personales para acceder a la red de la empresa o si desea limitar las opciones de conectividad para las aplicaciones de trabajo, puede restringir las opciones de conexión.
iOS, macOS, Android y Win	Tanto las aplicaciones de trabajo como las personales pueden utilizar los perfiles de Wi-Fi guardados en el dispositivo para conectarse a la red de la empresa.

Creación de un perfil de Wi-Fi

La configuración del perfil obligatorio varía para cada tipo de dispositivo y depende del tipo de seguridad Wi-Fi y del protocolo de autenticación que seleccione.

Antes de empezar:

- Si los dispositivos utilizan la autenticación basada en certificados para conexiones Wi-Fi de trabajo, cree un perfil de certificado de CA y asígnelo a las cuentas de usuario, a los grupos de usuarios o a los grupos de dispositivos. Para enviar certificados de cliente a dispositivos, cree un SCEP, un certificado compartido o un perfil de credenciales de usuario para asociarlo al perfil Wi-Fi.
- Para los dispositivos BlackBerry 10, iOS, macOS, Android con perfiles de trabajo o dispositivos Samsung KNOX que utilizan un servidor proxy para las conexiones Wi-Fi de trabajo, cree un perfil de proxy para asociarlo al perfil de Wi-Fi.
- Si los dispositivos con BlackBerry 10 utilizan una VPN para las conexiones Wi-Fi de trabajo, cree un perfil de VPN para asociarlo al perfil Wi-Fi.

1. En la barra de menú, haga clic en **Políticas y perfiles**.
2. Haga clic en **Redes y conexiones > Wi-Fi**.
3. Haga clic en +.

4. Escriba un nombre y una descripción para el perfil de Wi-Fi. Dicha información se muestra en los dispositivos.
5. En el campo **SSID**, escriba el nombre de red de una red Wi-Fi.
6. Si la red Wi-Fi no difunde el SSID, seleccione la casilla de verificación **Red oculta**.
7. Opcionalmente, desactive la casilla de verificación para cualquier tipo de dispositivo para el que no desee configurar el perfil.
8. Realice las acciones siguientes:
   a) Haga clic en la pestaña de un tipo de dispositivo.
   b) Configure los valores adecuados para cada configuración del perfil para que coincida con la configuración Wi-Fi del entorno de la empresa. Si la empresa requiere que los usuarios proporcionen un nombre de usuario y una contraseña para conectarse a la red Wi-Fi y el perfil es para varios usuarios, en el campo **Nombre de usuario** escriba `%UserName%`.

   Para obtener más información acerca de la configuración de cada perfil, consulte Ajustes del perfil de Wi-Fi.
9. Repita el paso 7 para cada tipo de dispositivo en la empresa.
10. Haga clic en **Agregar**.

Conceptos relacionados

Envío de certificados a dispositivos mediante perfiles
Ajustes del perfil de Wi-Fi

Tareas relacionadas

Asignación de un perfil o una política de TI a un grupo de usuarios
Asignar un perfil o una política de TI a una cuenta de usuario

Configuración de las VPN de trabajo para dispositivos

Puede utilizar un perfil de VPN para especificar cómo los dispositivos con BlackBerry 10, iOS, macOS, Samsung KNOX Workspace y Windows 10 se conectan a una VPN de trabajo. Se puede asignar un perfil de VPN a cuentas de usuarios, a grupos de usuarios y a grupos de dispositivos. En los dispositivos con BlackBerry 10, también puede asociar un perfil de VPN con un perfil de Wi-Fi.

Para conectarse a una VPN de trabajo, los usuarios de Windows Phone y dispositivos Android, que no sean dispositivos Samsung KNOX Workspace, deben configurar manualmente un perfil de VPN en los dispositivos.

Dispositivo	Aplicaciones y conexiones de red
BlackBerry 10	• De forma predeterminada, tanto las aplicaciones de trabajo como las personales pueden utilizar los perfiles VPN guardados en el dispositivo para conectarse a la red de la empresa. Las aplicaciones de trabajo también pueden utilizar BlackBerry Infrastructure para conectarse a la red de la empresa. Si los estándares de seguridad de la empresa no permiten aplicaciones personales para acceder a la red de la empresa o si desea limitar las opciones de conectividad para las aplicaciones de trabajo, puede restringir las opciones de conexión.

Dispositivo	Aplicaciones y conexiones de red
iOS	• Tanto las aplicaciones de trabajo como las personales pueden utilizar los perfiles VPN guardados en el dispositivo para conectarse a la red de la empresa. Puede activar una VPN por aplicación para que un perfil de VPN limite el perfil de las aplicaciones de trabajo que se especifiquen.
macOS	• Puede configurar perfiles de VPN para permitir que las aplicaciones se conecten a la red de la empresa.
KNOX Workspace	• Las aplicaciones de trabajo pueden utilizar los perfiles VPN guardados en el dispositivo para conectarse a la red de la empresa. • Puede activar una VPN por aplicación para limitar el perfil de las aplicaciones de trabajo que se especifiquen. • Una aplicación de cliente VPN compatible debe estar instalada en el dispositivo. Cisco AnyConnect y Juniper son compatibles. **Nota:** La aplicación Juniper solo es compatible con SSL VPN.
Windows 10	• Puede configurar perfiles de VPN para permitir que las aplicaciones se conecten a la red de la empresa. En el perfil de VPN, puede especificar una lista de aplicaciones que debe utilizar la VPN.

Crear un perfil VPN

La configuración del perfil obligatorio varía para cada tipo de dispositivo y depende del tipo de conexión VPN y del tipo de autenticación que seleccione.

Nota: Algunos dispositivos pueden no ser capaces de guardar la contraseña xAuth. Para obtener más información, visite support.blackberry.com/kb y lea el artículo KB30353.

Antes de empezar:

- Si los dispositivos utilizan la autenticación basada en certificados para conexiones VPN de trabajo, cree un perfil de certificado de CA y asígnelo a las cuentas de usuario, a los grupos de usuarios o a los grupos de dispositivos. Para enviar certificados de cliente a dispositivos, cree un perfil de credenciales de usuario, SCEP o certificado compartido para asociarlo al perfil de VPN.
- Para los dispositivos con BlackBerry 10, iOS, macOS y Samsung KNOX Workspace que utilizan un servidor proxy, cree un perfil de proxy para asociarlo al perfil de VPN. (El servidor proxy para los dispositivos con Windows 10 se configura en el perfil de VPN).
- Para dispositivos con KNOX Workspace, agregue la aplicación de cliente VPN apropiada a la lista de aplicaciones y asígnela a las cuentas de usuario, a los grupos de usuarios o a los grupos de dispositivos. Las aplicaciones de cliente VPN admitidas son Cisco AnyConnect y Juniper.

1. En la barra de menú, haga clic en **Políticas y perfiles**.
2. Haga clic en **Redes y conexiones > VPN**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil VPN. Dicha información se muestra en los dispositivos.
5. Opcionalmente, desactive la casilla de verificación para cualquier tipo de dispositivo para el que no desee configurar el perfil.
6. Realice las acciones siguientes:
   a) Haga clic en la pestaña de un tipo de dispositivo.

b) Configure los valores adecuados para cada configuración del perfil para que coincida con la configuración de la red VPN del entorno de la empresa. Si la empresa requiere que los usuarios proporcionen un nombre de usuario y una contraseña para conectarse a la VPN y el perfil es para varios usuarios, en el campo **Nombre de usuario** escriba `%UserName%`.

Para obtener más información acerca de la configuración de cada perfil, consulte Configuración de perfil VPN.

7. Repita el paso 5 para cada tipo de dispositivo en la empresa.
8. Haga clic en **Agregar**.

Conceptos relacionados

Envío de certificados a dispositivos mediante perfiles
Configuración de perfil VPN

Tareas relacionadas

Asignación de un perfil o una política de TI a un grupo de usuarios
Asignar un perfil o una política de TI a una cuenta de usuario

Activación de VPN a petición para dispositivos iOS o macOS

La VPN a petición le permite especificar si un dispositivo iOS o macOS puede conectarse automáticamente a una red VPN en un dominio concreto. Los certificados de cliente proporcionan autenticación al dispositivo del usuario cuando se accede a un dominio concreto. Por ejemplo, puede especificar el dominio de la empresa para que los usuarios puedan acceder al contenido de su intranet mediante una VPN a petición.

Referencia relacionada

iOS y macOS: configuración del perfil de VPN

Activación de una VPN por aplicación

Puede configurar VPN por aplicación en los dispositivos iOS, Samsung KNOX Workspace y Windows 10 para especificar qué aplicaciones en los dispositivos deben utilizar una VPN para sus datos en tránsito. La VPN por aplicación ayuda a disminuir la carga de la VPN de su empresa al permitir que solo determinado tráfico de trabajo utilice la VPN (por ejemplo, al acceder a servidores de aplicaciones o páginas web detrás del firewall). Esta característica también es compatible con la privacidad del usuario y aumenta la velocidad de conexión de las aplicaciones personales al no enviar el tráfico personal a través de la VPN.

Para los dispositivos iOS, las aplicaciones se asocian a un perfil de VPN cuando asigna la aplicación o grupo de aplicaciones a un usuario, grupo de usuarios o grupo de dispositivos.

Para los dispositivos con Samsung KNOX Workspace, las aplicaciones se agregan a la configuración "Aplicaciones que pueden utilizar la conexión VPN" en el perfil de VPN.

Para los dispositivos con Windows 10, las aplicaciones se agregan a la configuración "Lista de activadores de la aplicación" en el perfil de VPN.

Referencia relacionada

iOS y macOS: configuración del perfil de VPN
Android: ajustes del perfil de VPN

Windows 10: ajustes del perfil de VPN

¿Cómo BlackBerry UEM elige qué ajustes de VPN por aplicación se asignan a dispositivos iOS ?

Solo se puede asignar un perfil de VPN a una aplicación o grupo de aplicaciones. BlackBerry UEM utiliza las siguientes reglas para determinar qué ajustes de VPN por aplicación asignar a una aplicación en los dispositivos iOS:

- Los ajustes de VPN por aplicación que se asocian directamente a una aplicación tienen prioridad sobre los ajustes de VPN por aplicación asociados indirectamente a un grupo de aplicaciones.
- Los ajustes de VPN por aplicación que se asocian directamente a un usuario tienen prioridad sobre los ajustes de VPN por aplicación asociados indirectamente a un grupo de usuarios.
- Los ajustes de VPN por aplicación que se asignan a una aplicación obligatoria tienen prioridad sobre los ajustes de VPN por aplicación asignados a una instancia opcional de la misma aplicación.
- Los ajustes de VPN por aplicación que se asocian al nombre del grupo de usuarios que aparece anteriormente en la lista alfabética tienen prioridad si se cumplen las siguientes condiciones:
  - Se asigna una aplicación a varios grupos de usuarios
  - La misma aplicación aparece en los grupos de usuarios
  - Se asigna la aplicación del mismo modo, ya sea como una sola aplicación o como un grupo de aplicaciones
  - La aplicación tiene la misma disposición en todas las asignaciones, ya sea obligatoria u opcional

  Por ejemplo, puede asignar Cisco WebEx Meetings como una aplicación opcional a los grupos de usuarios de desarrollo y marketing. Cuando un usuario se encuentra en ambos grupos, los ajustes de VPN por aplicación para el grupo de desarrollo se aplican a la aplicación WebEx Meetings para dicho usuario.

Si el perfil de VPN por aplicación se asigna a un grupo de dispositivos, tiene prioridad sobre el perfil de VPN por aplicación que se asigna a la cuenta de usuario para los dispositivos que pertenecen al grupo de dispositivos.

Configuración de los perfiles de proxy para dispositivos

Puede especificar la forma de uso de un servidor proxy de los dispositivos para acceder a servicios web en Internet o en una red de trabajo. Para los dispositivos con BlackBerry 10, iOS, macOS y Android se crea un perfil de proxy. Para los dispositivos con Windows 10, puede agregar los ajustes de proxy en el perfil de Wi-Fi o de VPN.

A menos que se indique lo contrario, los perfiles de proxy son compatibles con los servidores proxy con autenticación básica o sin ella.

Dispositivo	Configuración de proxy
BlackBerry 10	Cree un perfil de proxy y asócielo con los perfiles que utiliza la empresa, que puede incluir cualquiera de los siguientes: • Wi-Fi • VPN • Conectividad de la empresa

Dispositivo	Configuración de proxy
iOS	Cree un perfil de proxy y asócielo con los perfiles que utiliza la empresa, que puede incluir cualquiera de los siguientes: • Wi-Fi • VPN También se puede asignar un perfil de proxy a cuentas de usuarios, a grupos de usuarios y a grupos de dispositivos. **Nota:** Un perfil de proxy que se asigna a cuentas de usuario, a grupos de usuarios o a grupos de dispositivos es un proxy global para los dispositivos supervisados únicamente y tiene prioridad sobre un perfil de proxy que esté asociado a un perfil de Wi-Fi o de VPN. Los dispositivos supervisados utilizarán la configuración de proxy global para todas las conexiones HTTP.
macOS	Cree un perfil de proxy y asócielo a un perfil Wi-Fi o de VPN. macOS aplica perfiles a las cuentas de usuario o los dispositivos. Los perfiles de proxy se aplican a los dispositivos.
Android	Para dispositivos Android con un perfil de trabajo, cree un perfil de proxy y asócielo a un perfil de Wi-Fi. Los dispositivos Android 8.0 y versiones posteriores con Controles de MDM o Privacidad del usuario no son compatibles con perfiles de Wi-Fi con configuración de proxy. Si un dispositivo con uno de estos tipos de activación se actualiza a Android 8.0, los perfiles de Wi-Fi que tienen un perfil de proxy asociado se eliminarán del dispositivo.

Dispositivo	Configuración de proxy
Samsung KNOX	Cree un perfil de proxy y asócielo a los perfiles que utiliza la empresa. Se aplican las siguientes condiciones: • Para los perfiles Wi-Fi, solo los perfiles de proxy con la configuración manual son compatibles con los dispositivos KNOX. Los perfiles de proxy que se asocien a los perfiles de Wi-Fi son compatibles con los servidores proxy con autenticación básica, NTLM o sin autenticación. • Para los perfiles VPN y de conectividad de la empresa, los perfiles de proxy con la configuración manual son compatibles con los dispositivos Samsung KNOX Workspace que utilizan KNOX 2.5 y una versión posterior. Los perfiles de proxy con la configuración de PAC son compatibles con los dispositivos KNOX Workspace que utilizan una versión de KNOX posterior a la 2.5. **Nota:** Para utilizar perfil de proxy con un perfil de conectividad de la empresa,BlackBerry Secure Connect Plus debe estar activado. También se puede asignar un perfil de proxy a cuentas de usuarios, a grupos de usuarios y a grupos de dispositivos. Se aplican las siguientes condiciones: • En los dispositivos KNOX Workspace, el perfil configura las opciones de proxy del navegador en el espacio de trabajo. • En los dispositivos con Samsung KNOX MDM, el perfil configura las opciones de proxy del navegador en el dispositivo. **Nota:** La Configuración de PAC no es compatible con los dispositivos KNOX Workspace que utilizan KNOX 2.5 y versiones anteriores y con los dispositivos con KNOX MDM.
Windows 10	Cree un perfil de Wi-Fi o de VPN y especifique la información del servidor proxy en los ajustes del perfil. Se aplican las siguientes condiciones: • Proxy Wi-Fi solo admite la configuración manual y únicamente es compatible con los dispositivos con Windows 10 Mobile. • Proxy VPN admite PAC o configuración manual.

Creación de un perfil de proxy

Si la empresa utiliza un archivo PAC para definir las reglas de proxy, puede seleccionar la configuración de PAC para utilizar el servidor proxy desde el archivo PAC que especifique. De lo contrario, puede seleccionar la configuración manual y especificar la configuración del servidor proxy directamente en el perfil.

1. En la barra de menú, haga clic en **Políticas y perfiles**.
2. Haga clic en **Redes y conexiones > Proxy**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil de proxy.
5. Haga clic en la pestaña de un tipo de dispositivo.
6. Lleve a cabo una de las tareas siguientes:

Tarea	Pasos
Especificar los ajustes de configuración de PAC	**a.** En la lista desplegable **Tipo**, compruebe que está seleccionada la opción **Configuración de PAC**. **b.** En el campo **URL de PAC**, escriba la URL para el servidor web que aloja el archivo de PAC e incluya el nombre del archivo (por ejemplo, http://www.example.com/PACfile.pac). El archivo PAC no debe alojarse en un servidor que aloje BlackBerry UEM ni ninguno de sus componentes. **c.** En la pestaña **BlackBerry**, lleve a cabo las acciones siguientes: **1.** Si la empresa requiere que los usuarios proporcionen un nombre de usuario y una contraseña para conectarse al servidor proxy y el perfil es para varios usuarios, en el campo **Nombre de usuario** escriba `%UserName%`. Si el servidor proxy solicita el nombre de dominio para la autenticación, utilice el formato *<dominio>**<nombre de usuario>*. **2.** En la lista desplegable **El usuario puede editar**, haga clic en los ajustes de proxy que los usuarios de dispositivos con BlackBerry 10 pueden cambiar. La configuración predeterminada es **Solo lectura**.
Especificar los ajustes de configuración manual	**a.** En la lista desplegable **Tipo**, haga clic en **Configuración manual**. **b.** En el campo **Host**, escriba la dirección FQDN o IP del servidor proxy. **c.** En el campo **Puerto**, escriba el número de puerto del servidor proxy. **d.** Si la empresa requiere que los usuarios proporcionen un nombre de usuario y una contraseña para conectarse al servidor proxy y el perfil es para varios usuarios, en el campo **Nombre de usuario** escriba `%UserName%`. Si el servidor proxy solicita el nombre de dominio para la autenticación, utilice el formato *<dominio>**<nombre de usuario>*. **e.** En la pestaña **BlackBerry**, lleve a cabo las acciones siguientes: **1.** En la lista desplegable **El usuario puede editar**, haga clic en los ajustes de proxy que los usuarios de dispositivos con BlackBerry 10 pueden cambiar. La configuración predeterminada es **Solo lectura**. **2.** Opcionalmente, puede especificar una lista de direcciones a las que los usuarios puedan acceder directamente desde los dispositivos con BlackBerry 10 sin utilizar el servidor proxy. En el campo **Lista de exclusión**, escriba las direcciones (FQDN o IP) y utilice un punto y coma (;) para separar los valores de la lista. Puede utilizar el carácter comodín (*) en un FQDN o IP (por ejemplo, *.ejemplo.com o 192.0.2.*).

7. Repita los pasos 4 y 5 para cada tipo de dispositivo en la empresa.
8. Haga clic en **Agregar**.

Después de terminar:

- Asocie el perfil de proxy con un perfil de Wi-Fi, de VPN o de conectividad de la empresa.

- Si fuera necesario, clasifique los perfiles. La clasificación que se especifique solo se aplicará si se asigna un perfil de proxy a los grupos de usuarios o de dispositivos.

Tareas relacionadas

Asignación de un perfil o una política de TI a un grupo de usuarios
Asignar un perfil o una política de TI a una cuenta de usuario

Uso de la conectividad de la empresa y BlackBerry Secure Connect Plus en las conexiones con los recursos de trabajo

Puede utilizar un perfil de conectividad de la empresa para activar la conectividad de la empresa y BlackBerry Secure Connect Plus para los dispositivos compatibles.

Conectividad de empresa

La conectividad de empresa envía todos los datos de trabajo enviados entre los dispositivos con BlackBerry 10 y la red de su empresa a través de BlackBerry Infrastructure a BlackBerry UEM. Esta función le permite evitar la apertura de una conexión directa a través del firewall de la empresa a Internet para la gestión de dispositivos con BlackBerry 10 y las aplicaciones que se conectan al servidor de correo, a la CA interna y a otros servidores web o servidores de contenido. La conectividad de la empresa siempre está activada para los dispositivos con BlackBerry 10, aunque no utilice BlackBerry Secure Connect Plus. Dichos dispositivos eligen la ruta más eficiente basándose en la disponibilidad de la red.

BlackBerry Secure Connect Plus

BlackBerry Secure Connect Plus es un componente de BlackBerry UEM que proporciona un túnel IP seguro entre las aplicaciones y la red de la empresa:

- En los dispositivos con BlackBerry 10 y Android con un perfil de trabajo, todas las aplicaciones de trabajo utilizan el túnel seguro.
- En los dispositivos Samsung KNOX Workspace, puede permitir que todas las aplicaciones de espacio de trabajo utilicen el túnel o especificar aplicaciones mediante una VPN por aplicación.
- En los dispositivos iOS, puede permitir que todas las aplicaciones utilicen el túnel o especificar aplicaciones mediante una VPN por aplicación.

Nota: Si BlackBerry Secure Connect Plus no está disponible en su región, debe desactivarlo manualmente para los dispositivos Android en el perfil de conectividad de la empresa.

Este túnel IP seguro proporciona a los usuarios acceso a los recursos de trabajo detrás del firewall de la empresa, lo que garantiza que los datos estén protegidos mediante protocolos estándar y cifrado integral.

BlackBerry Secure Connect Plus y un dispositivo compatible establecen un túnel IP seguro cuando se trata de la mejor opción disponible para realizar la conexión a la red de la empresa. Si se asigna un perfil Wi-Fi o un perfil VPN a un dispositivo y el dispositivo puede acceder a la red Wi-Fi o VPN del trabajo, el dispositivo utilizará estos métodos para conectarse a la red. Si estas opciones no están disponibles (por ejemplo, si el usuario no se encuentra dentro del alcance de la red Wi-Fi del trabajo), BlackBerry Secure Connect Plus y el dispositivo establecerán un túnel IP seguro.

En los dispositivos iOS, si configura una red VPN por aplicación para BlackBerry Secure Connect Plus, las aplicaciones configuradas siempre utilizarán una conexión de túnel segura a través de BlackBerry Secure Connect Plus, incluso si la aplicación puede conectarse a la red Wi-Fi de trabajo o VPN especificada en un perfil de Wi-Fi o de VPN.

Los dispositivos compatibles se comunican con BlackBerry UEM para establecer un túnel seguro a través de BlackBerry Infrastructure. Se establece un túnel para cada dispositivo. El túnel es compatible con protocolos IPv4 estándar (TCP y UDP). Mientras el túnel esté abierto, las aplicaciones puede acceder a los recursos de la red. Cuando el túnel ya no sea necesario (por ejemplo, si el usuario se encuentra dentro del alcance de la red Wi-Fi del trabajo), se dará por finalizado.

BlackBerry Secure Connect Plus ofrece las siguientes ventajas:

- El tráfico IP que se envía entre los dispositivos y BlackBerry UEM se somete a un cifrado integral mediante AES256, lo que garantiza la seguridad de los datos de trabajo.
- BlackBerry Secure Connect Plus proporciona una conexión segura y de confianza a los recursos del trabajo cuando el usuario del dispositivo no puede acceder a la red Wi-Fi del trabajo ni a la VPN.
- BlackBerry Secure Connect Plus se instala detrás del firewall de la empresa, de modo que los datos se transmiten a través de una zona de confianza que sigue los estándares de seguridad de la empresa.
- BlackBerry Secure Connect Plus proporciona la opción de implementar un transcodificador para dispositivos con BlackBerry 10 que permitan el cifrado personalizado de los datos que pasan a través del túnel seguro.

Para obtener más información acerca de cómo laconectividad de la empresa y BlackBerry Secure Connect Plus transfieren datos hacia y desde los dispositivos, consulte el contenido de Arquitectura.

Pasos para activar BlackBerry Secure Connect Plus

Para activar BlackBerry Secure Connect Plus, siga los pasos siguientes:

Paso	Acción
1	Verifique que el dominio de BlackBerry UEM de la empresa cumple los requisitos para utilizar BlackBerry Secure Connect Plus .
2	Verifique que BlackBerry Secure Connect Plus esté activado en el perfil de conectividad de la empresa predeterminado o en un perfil de conectividad de la empresa personalizado que haya creado.
3	De manera opcional, especifique la configuración DNS adecuada para la aplicación BlackBerry Connectivity.
4	Si su entorno incluye dispositivos Android con un perfil de trabajo y dispositivos Samsung KNOX Workspace activados con BlackBerry Dynamics, optimice las conexiones de túnel seguras.
5	Asigne el perfil de conectividad de la empresa a usuarios y grupos.

Requisitos del servidor y del dispositivo

Para utilizar BlackBerry Secure Connect Plus, el entorno de la empresa debe cumplir con los requisitos siguientes.

Para el dominio de BlackBerry UEM:

- El firewall de la empresa debe permitir conexiones salientes a través del puerto 3101 a <*región*>.turnb.bbsecure.com y <*región*>.bbsecure.com. Si configura BlackBerry UEM para que utilice un servidor proxy, verifique que dicho servidor permita conexiones a estos subdominios a través del puerto 3101. Para obtener más información acerca de los dominios y las direcciones IP que puede utilizar en el firewall, vaya a http://support.blackberry.com/kb y consulte el artículo KB36470.

- En cada instancia de BlackBerry UEM, el componente de BlackBerry Secure Connect Plus debe estar ejecutándose.
- De forma predeterminada, los dispositivos Android que tienen un perfil de trabajo tienen restringido el uso de BlackBerry Secure Connect Plus para conectarse a Google Play y los servicios subyacentes (com.android.providers.media, com.android.vending y com.google.android.apps.gcs). Google Play no cuenta con compatibilidad de proxy. Los dispositivos Android que tienen un perfil de trabajo utilizan una conexión directa a través de Internet a Google Play.

  Estas restricciones están configuradas en el perfil de conectividad de la empresa predeterminado y en cualquier perfil de conectividad de la empresa nuevo que cree. Se recomienda mantener estas restricciones. Si elimina estas restricciones, debe ponerse en contacto con el soporte de Google Play para conocer la configuración de cortafuegos necesaria para permitir las conexiones a Google Play mediante BlackBerry Secure Connect Plus.

Nota: Si su entorno incluye dispositivos con KNOX Workspace y Android con perfiles de trabajo y aplicaciones de BlackBerry Dynamics, consulte Optimización de las conexiones de túnel seguras para dispositivos Android que utilizan aplicaciones de BlackBerry Dynamics.

En los dispositivos compatibles:

Dispositivo	Requisitos

BlackBerry 10	• BlackBerry 10 Versión 10.3.2 de OS o posteriores
	• Cualquiera de los tipos de activación siguientes:
	  • Trabajo y personal - Empresa
	  • Solo espacio de trabajo
	  • Trabajo y personal - Regulado

Samsung KNOX Workspace	• Android 5.0 o posteriores
	• Samsung KNOX MDM 5.0 o posteriores
	• Samsung KNOX 2.3 o posteriores
	• Cualquiera de los tipos de activación siguientes:
	  • Solo espacio de trabajo (Samsung KNOX)
	  • Trabajo y personal: control total (Samsung KNOX)
	  • Trabajo y personal: privacidad de usuario (Samsung KNOX)

Dispositivos Android que utilizan un perfil de trabajo	• Android 5.1 o posteriores
	• Cualquiera de los tipos de activación siguientes:
	  • Solo espacio de trabajo (Premium)
	  • Trabajo y personal: privacidad de usuario (Premium)

iOS	• iOS 9 o posteriores • Los dispositivos deben activarse mediante BlackBerry UEM Client, disponible en App Store • Tipo de activación de Controles de MDM

Si desea obtener más información acerca de las licencias que se requieren para utilizar BlackBerry Secure Connect Plus, consulte el contenido referente a Licencias.

Equilibrio de carga y alta disponibilidad de BlackBerry Secure Connect Plus

Si un dominio incluye más de una instancia de BlackBerry UEM, el componente de BlackBerry Secure Connect Plus de cada instancia ejecuta y procesa datos. Los datos se cargan de forma equilibrada en todos los componentes de BlackBerry Secure Connect Plus del dominio.

La conmutación por error de alta disponibilidad está disponible para dispositivos BlackBerry 10, Samsung KNOX Workspace y Android que utilizan un perfil de trabajo y dispositivos iOS. Si un dispositivo está utilizando un túnel seguro y el componente de BlackBerry Secure Connect Plus actual deja de estar disponible, BlackBerry Infrastructure asignará el dispositivo a un componente de BlackBerry Secure Connect Plus de otra instancia de BlackBerry UEM. El dispositivo reanuda la utilización del túnel seguro con una interrupción mínima.

BlackBerry Secure Connect Plus y BlackBerry Connectivity Node

Puede instalar una o más instancias de BlackBerry Connectivity Node para agregar las instancias adicionales de los componentes de conectividad del dispositivo al dominio de su empresa. Cada BlackBerry Connectivity Node contiene una instancia activa de BlackBerry Secure Connect Plus que puede procesar los datos de dispositivo y establecer conexiones seguras.

También puede crear grupos de servidores. Un grupo de servidores contiene una o más instancias de BlackBerry Connectivity Node. Al crear un grupo de servidores, debe especificar la ruta de datos regionales que desea que los componentes usen para conectarse a BlackBerry Infrastructure. Por ejemplo, puede crear un grupo de servidores para dirigir las conexiones de dispositivo para BlackBerry Secure Connect Plus y BlackBerry Secure Gateway para usar la ruta de Estados Unidos a BlackBerry Infrastructure. Puede asociar perfiles de correo y de conectividad de empresa con un grupo de servidores. Cualquier dispositivo que se asigne a estos perfiles usa la conexión regional del grupo de servidores a BlackBerry Infrastructure cuando utiliza cualquiera de los componentes de BlackBerry Connectivity Node.

Si un grupo de servidores contiene varias instancias de BlackBerry Connectivity Node, los dispositivos pueden utilizar cualquier instancia que se esté ejecutando. Se realiza una carga equilibrada de las conexiones de dispositivo entre las instancias disponible en el grupo. Si no hay instancias disponibles, los dispositivos no pueden usar esos componentes para las conexiones seguras. Debe estar disponible al menos una de las instancias.

Para obtener más información sobre la planificación y la instalación de un BlackBerry Connectivity Node, consulte el contenido sobre Planificación de contenido y el contenido de instalación y de actualización

Activación y configuración de la conectividad de la empresa y BlackBerry Secure Connect Plus

Puede usar un perfil de conectividad de la empresa para activar la conectividad de la empresa y BlackBerry Secure Connect Plus.

- Los dispositivos con BlackBerry 10 admiten la conectividad de la empresa con y sin BlackBerry Secure Connect Plus. No puede desactivar la conectividad de la empresa de los dispositivos con BlackBerry 10.
- Los dispositivos Android con un perfil de trabajo, los dispositivos Samsung KNOX Workspace y los dispositivos iOS son compatibles con conectividad de empresa a través de BlackBerry Secure Connect Plus.

Nota: Si utiliza un perfil de correo para activar BlackBerry Secure Gateway para dispositivos iOS, se recomienda configurar una VPN por aplicación para BlackBerry Secure Connect Plus. Para obtener más información acerca de BlackBerry Secure Gateway, consulte Protección de datos de correo electrónico mediante BlackBerry Secure Gateway.

Nota: Si su entorno incluye dispositivos Android con un perfil de trabajo y dispositivos Samsung KNOX Workspace con aplicaciones de BlackBerry Dynamics, consulte Optimización de las conexiones de túnel seguras para dispositivos Android que utilizan aplicaciones de BlackBerry Dynamics.

Creación de un perfil de conectividad de la empresa

Si desea utilizar un perfil de conectividad de la empresa para configurar BlackBerry Secure Connect Plus, consulte Activar BlackBerry Secure Connect Plus en lugar de esta tarea.

De forma predeterminada, BlackBerry UEM asigna el perfil de conectividad de la empresa predeterminado a todos los usuarios. Puede editar el perfil predeterminado o crear nuevos perfiles de conectividad de la empresa.

Antes de empezar: Si es necesario, cree un perfil de proxy.

1. En la barra de menú, haga clic en **Políticas y perfiles**.
2. Haga clic en **Redes y conexiones > Conectividad de empresa**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil. Cada perfil de conectividad de la empresa debe tener un nombre único.
5. Realice las acciones siguientes:
   a) Haga clic en la pestaña de un tipo de dispositivo.
   b) Si está activada la conectividad de la empresa y utiliza un proxy, seleccione un perfil de proxy.
6. Repita el paso 4 para cada tipo de dispositivo compatible en la empresa.
7. Haga clic en **Agregar**.

Después de terminar: Si fuera necesario, clasifique los perfiles.

Conceptos relacionados

Configuración del perfil de conectividad de empresa

Tareas relacionadas

Asignación de un perfil o una política de TI a un grupo de usuarios
Asignar un perfil o una política de TI a una cuenta de usuario

Activar BlackBerry Secure Connect Plus

Si desea permitir que los dispositivos utilicen BlackBerry Secure Connect Plus, deberá activar BlackBerry Secure Connect Plus en un perfil de conectividad de la empresa y asignar el perfil a los usuarios y grupos. De forma predeterminada, BlackBerry Secure Connect Plus está activado en los dispositivos con BlackBerry 10 y en los dispositivos compatibles Android. En los dispositivos iOS, BlackBerry Secure Connect Plus no está activado de manera predeterminada.

Puede realizar una de las acciones siguientes:

- Verifique que BlackBerry Secure Connect Plus está activado en el perfil de conectividad de la empresa predeterminado para los tipos de dispositivo apropiados. Si una cuenta de usuario no tiene asignado directamente un perfil de conectividad de la empresa personalizado o a través de la pertenencia al grupo de usuarios, BlackBerry UEM asignará el perfil predeterminado.
- Cree un perfil de conectividad de la empresa personalizado mediante las instrucciones siguientes y asígnelo a los usuarios y grupos.

Al aplicar el perfil de conectividad de empresa al dispositivo después de la activación, BlackBerry UEM instala la aplicación BlackBerry Connectivity en el dispositivo (para dispositivos Android que utilizan un perfil de trabajo, la aplicación se instala automáticamente desde Google Play; para dispositivos iOS, la aplicación se instala

automáticamente desde App Store). En los dispositivos con BlackBerry 10, la aplicación está oculta y no requiere la interacción del usuario.

BlackBerry lanza nuevas versiones de la aplicación para permitir nuevas mejoras y funciones. Para obtener instrucciones sobre la actualización de la aplicación y recibir información acerca de los últimos problemas conocidos y resueltos, consulte las notas de la versión de la aplicación BlackBerry Connectivity.

1. En la consola de gestión, en la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Redes y conexiones > Conectividad de empresa**.
3. Haga clic en +.
4. Si ha creado y configurado uno o más grupos de servidores para dirigir el tráfico de BlackBerry Secure Connect Plus a un ruta regional específica a BlackBerry Infrastructure, en la lista desplegable **Grupo de servidores de BlackBerry Secure Connect Plus**, haga clic en el grupo de servidores correspondiente.
5. Configure los valores correspondientes de la configuración de perfil de cada tipo de dispositivo. Para obtener más información acerca de la configuración de cada perfil, consulte Configuración del perfil de conectividad de empresa.
6. Haga clic en **Agregar**.
7. Asigne el perfil a las cuentas de grupos o usuarios.
8. Si ha configurado VPN por aplicación para dispositivos iOS, al asignar una aplicación o grupo de aplicaciones, asócielo con el perfil de conectividad de la empresa adecuado.

Después de terminar:

- En los dispositivos Samsung KNOX Workspace y Android que utilizan un perfil de trabajo, la aplicación de BlackBerry Connectivity solicitará a los usuarios que la ejecuten como una VPN y que le permitan el acceso a las claves privadas del dispositivo. Instruya a los usuarios para aceptar las solicitudes. Los usuarios de dispositivos Samsung KNOX Workspace, Android que utilizan un perfil de trabajo y los dispositivos iOS pueden abrir la aplicación para ver el estado de la conexión. No se requiere ninguna otra acción de los usuarios.
- Si crea más de un perfil de conectividad de la empresa, clasifique los perfiles.
- Si desea implementar el cifrado personalizado de BlackBerry Secure Connect Plus, deberá completar las tareas de configuración adicionales antes de que los usuarios activen los dispositivos BlackBerry 10. Consulte "Implementación de cifrado personalizado".
- Si está solucionando un problema de conexión con un dispositivo con KNOX Workspace, un dispositivo Android que utiliza un perfil de trabajo o un dispositivo iOS, la aplicación permite al usuario enviar los registros del dispositivo a una dirección de correo del administrador (el usuario introduce una dirección de correo electrónico que usted debe proporcionar). Tenga en cuenta que los registros no son visibles con Winzip. Se recomienda utilizar otra utilidad como 7-Zip.

Conceptos relacionados

Configuración del perfil de conectividad de empresa

Tareas relacionadas

Asignación de un perfil o una política de TI a un grupo de usuarios
Asignar un perfil o una política de TI a una cuenta de usuario
Clasificar perfiles

Especificar la configuración del DNS adecuada para la aplicación de BlackBerry Connectivity

Puede especificar los servidores DNS que desea que la aplicación BlackBerry Connectivity utilice en las conexiones de túnel seguro. También puede especificar los sufijos de búsqueda de DNS. Si no se especifica la configuración DNS, la aplicación obtendrá las direcciones DNS del equipo que aloja el componente de BlackBerry Secure Connect Plus y el sufijo de búsqueda predeterminado será el dominio DNS de ese equipo.

Si crea o configura uno o más grupos de servidores para dirigir las conexiones de BlackBerry Secure Connect Plus a una ruta regional a BlackBerry Infrastructure, puede especificar la configuración de DNS determinada para cada grupo de servidores. Si lo hace, la configuración DNS de un grupo de servidores tiene prioridad sobre la configuración de DNS global que se especifique mediante los siguientes pasos. Para obtener más información acerca de la creación y configuración de grupos de servidores, consulte el contenido referente a Instalación y actualización.

1. En la barra de menús, haga clic en **Configuración**.
2. Haga clic en **Infraestructura > BlackBerry Secure Connect Plus**.
3. Seleccione la casilla de verificación **Configure manualmente los servidores DNS** y haga clic en +.
4. Escriba la dirección del servidor DNS con notación decimal con puntos (por ejemplo, 192.0.2.0). Haga clic en **Agregar**.
5. Si fuera necesario, repita los pasos 3 y 4 para agregar más servidores DNS. En la tabla **Servidores DNS**, haga clic en las flechas de la columna **Clasificación** para establecer la prioridad de los servidores DNS.
6. Si desea especificar los sufijos de búsqueda de DNS, realice los pasos siguientes:
   a) Seleccione la casilla de verificación **Gestionar los sufijos de búsqueda de DNS manualmente** y haga clic en +.
   b) Escriba el sufijo de búsqueda de DNS (por ejemplo, domain.com). Haga clic en **Agregar**.
7. Si fuera necesario, repita el paso 6 para agregar más sufijos de búsqueda de DNS. En la tabla **Sufijos de búsqueda de DNS**, haga clic en las flechas de la columna **Clasificación** para establecer la prioridad de los servidores DNS.
8. Haga clic en **Guardar**.

Optimización de las conexiones de túnel seguras para dispositivos Android que utilizan aplicaciones de BlackBerry Dynamics

Si activa BlackBerry Secure Connect Plus y su entorno incluye aplicaciones de BlackBerry Dynamics instaladas en dispositivos Android que tienen un perfil de trabajo o dispositivos Samsung KNOX Workspace, se recomienda configurar el perfil de conectividad de BlackBerry Dynamics asignado a estos dispositivos para desactivar BlackBerry Proxy. El uso simultáneo de BlackBerry Proxy y BlackBerry Secure Connect Plus puede retrasar la actividad de la red de las aplicaciones porque los datos se enrutan a ambos componentes de la red.

1. En la barra de menú, haga clic en **Políticas y perfiles**.
2. Haga clic en **Redes y conexiones > Conectividad de BlackBerry Dynamics**.
3. Seleccione el perfil que está asignado a los dispositivos Android con perfiles de trabajo y a los dispositivos Samsung KNOX Workspace.
4. Haga clic en ✎.
5. Desactive la casilla de verificación **Enrutar todo el tráfico**.
6. Haga clic en **Guardar**.

Referencia relacionada

Configuración del perfil de conectividad de BlackBerry Dynamics

Dirigir el tráfico del espacio de trabajo de BlackBerry 10 mediante BlackBerry Secure Connect Plus si está disponible una red de Wi-Fi

Si utiliza BlackBerry UEM para configurar un perfil de Wi-Fi y asignarlo a los dispositivos con BlackBerry 10, estos priorizarán la red de trabajo de Wi-Fi por encima de BlackBerry Secure Connect Plus. Si la red de trabajo de Wi-Fi no está disponible y los dispositivos no tienen asignado un perfil de VPN o no puede acceder a la VPN, los dispositivos utilizarán BlackBerry Secure Connect Plus. Tiene la opción de dirigir todo el tráfico del espacio de trabajo a través de BlackBerry Secure Connect Plus aunque los dispositivos puedan acceder a la red de trabajo de Wi-Fi. Puede optar por utilizar esta opción si los estándares de seguridad de su empresa impiden las conexiones de dispositivos a los recursos de trabajo a través de la red Wi-Fi.

Nota: Al activar esta función, todo el tráfico del espacio de trabajo que normalmente utilizará la red Wi-Fi de trabajo se dirige a través de una conexión segura a BlackBerry Infrastructure. Es posible que esta característica tenga un impacto sobre la utilización de datos y los costes de red de la empresa. Verifique que esta es la configuración preferida de la empresa antes de activar esta característica.

Antes de empezar: En la política de TI que se asigna a los usuarios del dispositivo con BlackBerry 10, verifique que no se haya seleccionado la regla de política de TI "Forzar control de acceso a la red para las aplicaciones de trabajo".

1. En la barra de menú, haga clic en **Políticas y perfiles**.
2. Haga clic en **Redes y conexiones > Wi-Fi**.
3. Haga clic en un perfil de Wi-Fi asignado a usuarios de dispositivos con BlackBerry 10.
4. Haga clic en .
5. En la pestaña **BlackBerry**, en la sección **Perfiles asociados**, seleccione la casilla de verificación **Utilice un perfil de conectividad de empresa con una conexión BlackBerry Secure Connect Plus para los datos de trabajo**.
6. Haga clic en **Guardar**.

Después de terminar: Si creó y asignó múltiples perfiles de Wi-Fi, repita esta tarea según sea necesario.

Referencia relacionada

BlackBerry 10: ajustes del perfil de Wi-Fi

Resolución de problemas de BlackBerry Secure Connect Plus

Tenga en cuenta las cuestiones siguientes si tiene problemas para configurar BlackBerry Secure Connect Plus.

El adaptador de BlackBerry Secure Connect Plus entra en un estado de "Red no identificada" y deja de funcionar

Causa

Este problema puede ocurrir si reinicia el equipo que aloja BlackBerry Secure Connect Plus.

Solución: Windows Server 2008 R2 y Windows Server 2008 R2 SP1

1. En Administrador del servidor, expanda **Funciones > Política de red y servicios de acceso**. Haga clic con el botón derecho en **Enrutamiento y acceso remoto** y en **Desactivar Enrutamiento y acceso remoto**.
2. Haga clic con el botón derecho en **Enrutamiento y acceso remoto** y en **Configurar y activar enrutamiento y acceso remoto**.
3. Para completar el asistente de configuración, seleccione estas opciones:

   a. En la pantalla **Configuración**, seleccione **Traducción de direcciones de red (NAT)**.
   b. En la pantalla **Conexión a Internet de NAT**, seleccione **Usar esta interfaz pública para conectarse a Internet**. Compruebe que BlackBerry Secure Connect Plus se muestre en la lista de interfaces de red.
4. Expanda **Funciones > Política de red y servicios de acceso > Enrutamiento y acceso remoto > IPv4** y haga clic en **NAT**. Abra las propiedades **Conexión de área local** y seleccione **Interfaz pública conectada a Internet** y **Activar NAT en este dispositivo**. Haga clic en **Aceptar.**
5. Abra las propiedades **BlackBerry Secure Connect Plus** y seleccione **Interfaz privada conectada a red privada**. Haga clic en **Aceptar.**
6. Haga clic con el botón derecho en **Enrutamiento y acceso remoto** y en **Todas las tareas > Reiniciar**.
7. En los servicios de Windows, reinicie el servicio **BlackBerry UEM: BlackBerry Secure Connect Plus**.

En Conexiones de red, el adaptador de BlackBerry Secure Connect Plus puede tardar unos minutos en mostrar una conexión correcta.

Descargue e instale la revisión del artículo de la base de conocimientos de Windows La funcionalidad NAT falla en un servidor RRAS basado en Windows Server 2008 R2 SP1.

Solución: Windows Server 2012

1. En el Administrador del servidor, haga clic en **Administrar > Agregar funciones y características**. Haga clic en **Siguiente** hasta llegar a la pantalla **Características**. Expanda **Herramientas de administración de servidor remoto > Herramientas de administración de función** y seleccione **Herramientas de administración de acceso remoto**. Complete el asistente para instalar las herramientas.
2. Haga clic en **Herramientas > Administración de acceso remoto**.
3. En **Configuración**, haga clic en **DirectAccess y VPN**.
4. En **VPN**, haga clic en **Abrir administración de RRAS**.
5. Haga clic con el botón derecho en el servidor de enrutamiento y acceso remoto y en **Desactivar enrutamiento y acceso remoto**.
6. Haga clic con el botón derecho en Enrutamiento y servidor de acceso remoto y en **Configurar y activar enrutamiento y acceso remoto**.
7. Para completar el asistente de configuración, seleccione estas opciones:
   a. En la pantalla **Configuración**, seleccione **Traducción de direcciones de red (NAT)**.
   b. En la pantalla **Conexión a Internet de NAT**, seleccione **Usar esta interfaz pública para conectarse a Internet**. Compruebe que BlackBerry Secure Connect Plus se muestre en la lista de interfaces de red.
8. Abra **Enrutamiento y acceso remoto >** <*nombre del servidor*> **> IPv4** y haga clic en **NAT**. Abra las propiedades **Conexión de área local** y seleccione **Interfaz pública conectada a Internet** y **Activar NAT en este dispositivo**. Haga clic en **Aceptar**.
9. Abra las propiedades **BlackBerry Secure Connect Plus** y seleccione **Interfaz privada conectada a red privada**. Haga clic en **Aceptar.**
10. Haga clic con el botón derecho en el servidor de enrutamiento y acceso remoto y en **Todas las tareas > Reiniciar**.
11. En los servicios de Windows, reinicie el servicio **BlackBerry UEM: BlackBerry Secure Connect Plus**.

Descargue e instale la revisión del artículo de la base de conocimientos de Windows La funcionalidad NAT falla en un servidor RRAS basado en Windows Server 2012.

BlackBerry Secure Connect Plus no se inicia

Causa posible

La configuración de TCP/IPv4 del adaptador de BlackBerry Secure Connect Plus podría no ser la correcto.

Solución posible

En**Conexiones de red > Adaptador de BlackBerry Secure Connect Plus > Propiedades > Protocolo de Internet versión 4 (TCP/IPv4) > Propiedades**, compruebe que**Utilizar la siguiente dirección IP**está activada, con los siguientes valores predeterminados:

- Dirección IP: 172.16.0.1
- Máscara de subred: 255.255.0.0

Si es necesario, corrija esta configuración y reinicie el servidor.

BlackBerry Secure Connect Plus deja de funcionar después de una actualización de BlackBerry UEM

Causa

Este problema puede ocurrir cuando el servidor no se ha reiniciado durante una actualización RRAS antes de que BlackBerry UEM se haya actualizado a la versión 12.7, lo que produce un error de configuración de enrutamiento/NAT durante la actualización.

Solución

1. Reinicie el servidor.
2. En los servicios de Windows, detenga el servicio **BlackBerry UEM: BlackBerry Secure Connect Plus**.
3. Como administrador, inicie Windows PowerShell (de 64 bits) o abra un símbolo del sistema.
4. Vaya a `<drive>:\Archivos de programa\BlackBerry\UEMSecureConnectPlus\config\blackberry\` y ejecute **configureRRAS.bat**
5. Vaya a `<drive>:\Archivos de programa\BlackBerry\UEMSecureConnectPlus\config\` y ejecute **configure-network-interface.cmd**
6. En los servicios de Windows, inicie el servicio **BlackBerry UEM: BlackBerry Secure Connect Plus**.

Presentación de los archivos de registro de BlackBerry Secure Connect Plus

Dos archivos de registro, ubicados de forma predeterminada en *<unidad>*:\Program Files\BlackBerry\UEM\Logs*<aaaammdd>* ,, registran datos acerca de BlackBerry Secure Connect Plus:

- BSCP: registra los datos sobre el componente del servidor de BlackBerry Secure Connect Plus
- BSCP-TS: registra los datos de registro para las conexiones con la aplicación BlackBerry Connectivity

En cada equipo que aloja una instancia de BlackBerry Connectivity Node, los archivos de registro de BlackBerry Secure Connect Plus se encuentran en *<unidad>*:\Program Files\BlackBerry\BlackBerry Connectivity Node\Logs*<aaaammdd>*.

Finalidad	Archivo de registro	Ejemplo
Compruebe que BlackBerry Secure Connect Plus esté conectado a BlackBerry Infrastructure	BSCP	2015-01-19T13:17:47.540-0500 - BSCP {TcpClientConnectorNio#2} logging.feature.bscp.service|logging.component.bscp.pss.bcp [{}] - DEBUG Received Ping from [id: 0x60bce5a3, /10.90.84.22:28231 => stratos.bcp.bblabs.rim.net/206.53.155.152:3101], responding with Pong.2015-01-19T13:18:22.989-0500 - BSCP {ChannelPinger#1} logging.feature.bscp.service|logging.component.bscp.pss.bcp [{}] - DEBUG Sending Ping to [id: 0xb4a1677a, /10.90.84.22:28232 => stratos.bcp.bblabs.rim.net/206.53.155.152:3101]

Finalidad	Archivo de registro	Ejemplo
Compruebe que BlackBerry Secure Connect Plus esté preparado para recibir llamadas de la aplicación de BlackBerry Connectivity de los dispositivos	BSCP-TS	47: [14:13:21.231312][][3][AsioTurnSocket-1] Connected, host=68-171-243-141.rdns.blackberry.net 48: [14:13:21.239312][][3][AsioTurnSocket-1] Creating TURN allocation 49: [14:13:21.405121][][3][AsioTurnSocket-1] TURN allocation created
Compruebe que los dispositivos estén utilizando el túnel seguro	BSCP-TS	74: [10:39:45.746926][][3][Tunnel-2FFEC51E] Sent: 2130.6 KB (1733), Received: 201.9 KB (1370), Running: 00:07:00.139249
Compruebe que BlackBerry Secure Connect Plus esté utilizando la configuración del transcodificador personalizada	BSCP	"configuration_def" : "com.rim.p2e.vpn.server.cipherSuite" }], "TRANSCODER", ["provider", { "configuration_def" : "com.rim.p2e.vpn.transcoder.provider" }, "server_library", { "configuration_def" : "com.rim.p2e.vpn.transcoder.server.library" }, "server_config_blob", { "configuration_def" : "com.rim.p2e.vpn.transcoder.server.configBlob" }]]
Compruebe que los dispositivos estén utilizando un transcodificador personalizado	BSCP-TS	37: [13:41:39.800371][][3][BlackBerry_1.0.0.1-25B212A5] Connected

Conceptos relacionados

Uso de archivos de registro

Configuración de conexiones de red para aplicaciones de BlackBerry Dynamics

Los perfiles de conectividad de BlackBerry Dynamics definen las conexiones de red, los dominios de Internet, los rangos de dirección IP y los servidores de aplicaciones a los que los dispositivos se pueden conectar cuando se usan aplicaciones de BlackBerry Dynamics.

BlackBerry UEM incluye un perfil de conectividad de BlackBerry Dynamics predeterminado con ajustes preconfigurados. Si no se asigna un perfil de conectividad de BlackBerry Dynamics a una cuenta o grupo de usuarios al que pertenece el usuario, BlackBerry UEM envía el perfil de conectividad de BlackBerry Dynamics predeterminado a los dispositivos de un usuario. BlackBerry UEM envía automáticamente un perfil de conectividad de BlackBerry Dynamics a un dispositivo cuando un usuario lo activa, cuando actualiza un perfil de conectividad de BlackBerry Dynamics asignado o cuando se asigna un perfil de conectividad de BlackBerry Dynamics diferente a la cuenta o dispositivo de un usuario.

Nota: Para empresas con un entorno independiente de BlackBerry Dynamics existente, los perfiles de conectividad que se configuraron en Good Control se sincronizan de Good Control a BlackBerry UEM cuando realiza la sincronización entre Good Control y BlackBerry UEM. Los perfiles de conectividad se asignarán automáticamente a los mismos usuarios en BlackBerry UEM. Para obtener más información sobre la sincronización de Good Control con BlackBerry UEM, consulte la Guía de configuración.

Creación de un perfil de conectividad de BlackBerry Dynamics

1. En la barra de menú, haga clic en **Políticas y perfiles**.
2. Haga clic en **Redes y conexiones > Conectividad de BlackBerry Dynamics**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil.
5. Configure los valores adecuados para la configuración del perfil. Para obtener más información acerca de la configuración de cada perfil, consulte Configuración del perfil de conectividad de BlackBerry Dynamics.
6. Para agregar un servidor de aplicaciones para una aplicación de BlackBerry Dynamics, consulte Adición de un servidor de aplicaciones a un perfil de conectividad de BlackBerry Dynamics.
7. Haga clic en **Agregar**.

Después de terminar: Si fuera necesario, clasifique los perfiles.

Tareas relacionadas

Asignación de un perfil o una política de TI a un grupo de usuarios
Asignar un perfil o una política de TI a una cuenta de usuario

Referencia relacionada

Configuración del perfil de conectividad de BlackBerry Dynamics

Enrutamiento de todos los datos de aplicaciones de BlackBerry Dynamics a través de BlackBerry Proxy

En el perfil de conectividad de BlackBerry Dynamics, puede especificar los servidores a los que las aplicaciones de BlackBerry Dynamics de sus usuarios pueden acceder a través del firewall utilizando BlackBerry Proxy.

Si selecciona la opción Distribuir todo el tráfico, todos los datos de las aplicaciones de BlackBerry Dynamics, independientemente del dominio o la subred, se enrutan a través de BlackBerry Proxy.

El enrutamiento de todo el tráfico a través de BlackBerry Proxy tiene las siguientes ventajas:

- Los navegadores web y las aplicaciones de BlackBerry Dynamics de los dispositivos se pueden conectar a cualquier servidor detrás del firewall al que pueda acceder BlackBerry Proxy.
- Puede supervisar fácilmente el tráfico de datos entre las aplicaciones de BlackBerry Dynamics y sus recursos.

Debe tener en cuenta las consideraciones siguientes si selecciona la opción Distribuir todo el tráfico:

- El establecimiento de conexiones a servidores en Internet puede tardar más tiempo.
- Si está utilizando un proxy web para permitir el acceso a sitios externos y ha configurado ajustes en el proxy para restringir determinados sitios, cuando seleccione la opción Distribuir todo el tráfico, también deberá configurar las propiedades del proxy en BlackBerry Proxy. De lo contrario, las aplicaciones no podrán acceder a sitios externos. Para obtener más información sobre la configuración de BlackBerry Proxy, consulte el contenido de Configuración.

- BlackBerry Access se puede configurar con un archivo PAC que determina los sitios admitidos. En ese caso, el archivo PAC determina la configuración de proxy y la opción Distribuir todo el tráfico no tiene efecto. Para obtener más información, consulte la Guía de administración de BlackBerry Access.

Adición de un servidor de aplicaciones a un perfil de conectividad de BlackBerry Dynamics

Si tiene una aplicación de BlackBerry Dynamics proporcionada desde un servidor de aplicaciones o servidor web, puede especificar el nombre de dicho servidor y la prioridad de los clústeres de BlackBerry Proxy utilizados para la comunicación.

1. En la barra de menú, haga clic en **Políticas y perfiles**.
2. Haga clic en **Redes y conexiones > Conectividad de BlackBerry Dynamics**.
3. Haga clic en el perfil de conectividad de BlackBerry Dynamics en el que desee agregar un servidor de aplicaciones.
4. Haga clic en .
5. En **Servidores de aplicaciones**, haga clic en **Agregar**.
6. Seleccione la aplicación de BlackBerry Dynamics para la que desea agregar un servidor de aplicaciones.
7. Haga clic en **Guardar**.
8. En la tabla de la aplicación, haga clic en .
9. En el campo **Servidor**, especifique el FQDN del servidor de aplicaciones.
10. En el campo **Puerto**, especifique el puerto del clúster de BlackBerry Proxy que se utiliza para acceder al servidor.
11. En la lista desplegable **Prioridad**, especifique la prioridad del clúster de BlackBerry Proxy que debe utilizarse para acceder al dominio.
12. En el la lista desplegable **Clúster principal de BlackBerry Proxy**, especifique el nombre del clúster de BlackBerry Proxy que desea establecer como el clúster principal.
13. En el la lista desplegable **Clúster secundario de BlackBerry Proxy**, especifique el nombre del clúster de BlackBerry Proxy que desea establecer como el clúster secundario.
14. Haga clic en **Guardar**.

Uso de BlackBerry 2FA para establecer conexiones seguras a los recursos cruciales

BlackBerry 2FA protege el acceso a los recursos críticos de su empresa mediante la autenticación de dos factores. BlackBerry 2FA utiliza una contraseña que los usuarios deben introducir, y una solicitud de seguridad en sus dispositivos móviles cada vez que intentan acceder a los recursos.

Usted administra BlackBerry 2FA desde la consola de administración de BlackBerry UEM, donde utiliza un perfil de BlackBerry 2FA para habilitar la autenticación de dos factores para sus usuarios. Para utilizar la versión más reciente de BlackBerry 2FA y sus características asociadas, tales como la autenticación previa y el autorrescate, sus usuarios deben tener el perfil de BlackBerry 2FA asignado. Para obtener más información, consulte el contenido de BlackBerry 2FA.

Configuración de la autenticación de registro único de los dispositivos

Puede activar los dispositivos con BlackBerry 10 y varios dispositivos iOS mediante un perfil de registro único para que se autentiquen automáticamente con dominios y servicios web en la red de la empresa. Después de asignar un perfil de registro único, se le solicitará al usuario un nombre de usuario y contraseña la primera vez que intente acceder a un dominio seguro que haya especificado. La información de inicio de sesión se guarda en el dispositivo del usuario y se utiliza automáticamente cuando el usuario intenta acceder a cualquiera de los dominios seguros especificados en el perfil. Cuando el usuario cambia la contraseña, se le solicitará la próxima vez que intente acceder a un dominio seguro.

También puede utilizar un perfil de registro único para especificar los dominios de confianza de los certificados que se envían a los dispositivos con BlackBerry 10 mediante un perfil SCEP. Después de especificar los dominios de confianza, los usuarios de BlackBerry 10 pueden seleccionar los certificados requeridos cuando acceden a un dominio de confianza.

Los perfiles de registro único son compatibles con los tipos de autenticación siguientes:

Tipo de autenticación	SO del dispositivo	Se aplica a
• Kerberos	iOS	• Navegador y aplicaciones • Puede restringir qué aplicaciones puede utilizar el perfil
	BlackBerry 10 OS	• El navegador y aplicaciones en el espacio de trabajo
• NTLM • especificar los dominios de confianza de certificados SCEP	BlackBerry 10 OS	• El navegador y aplicaciones en el espacio de trabajo

Las aplicaciones de BlackBerry Dynamics también son compatibles con autenticación Kerberos. Para obtener más información, consulte Configuración de Kerberos para aplicaciones de BlackBerry Dynamics.

Requisitos previos: uso de la autenticación de Kerberos para los dispositivos

Cuando se utiliza Kerberos en los dispositivos, no se solicitará a los usuarios la información de inicio de sesión cuando estos accedan a los recursos internos de la empresa desde el navegador y las aplicaciones en el espacio de trabajo si hay disponible un TGT válido en los dispositivos.

Para configurar la autenticación de Kerberos de dominios específicos, puede cargar el archivo de configuración de la empresa de Kerberos (krb5.conf). BlackBerry UEM es compatible con la implementación de Heimdal de Kerberos.

Compruebe que el archivo de configuración cumpla con los requisitos siguientes:

- La configuración de Kerberos debe utilizar TCP por defecto en vez de UDP. Utilice el prefijo tcp/ en los host KDC.
- Si la empresa utiliza VPN, la puerta de enlace VPN debe permitir el tráfico a los KDC.

Para obtener más información acerca de la configuración de la autenticación Kerberos para aplicaciones de BlackBerry Dynamics, consulteConfiguración de Kerberos para aplicaciones de BlackBerry Dynamics.

Autenticación basada en certificados de iOS 8 y posteriores

En los dispositivos que ejecutan iOS 8.0 y versiones posteriores, se pueden utilizar certificados para autenticar los dispositivos iOS con dominios y servicios web en la red de la empresa. Puede agregar un perfil de certificado compartido, un perfil SCEP o un perfil de credenciales de usuario a un perfil de registro único. Cuando el navegador o las aplicaciones de los dispositivos iOS utilizan registros únicos basados en certificados, los usuarios se autentican automáticamente (siempre que el certificado sea válido) y no tienen que introducir la información de inicio de sesión cuando acceden a los dominios seguros especificados.

Conceptos relacionados

Envío del mismo certificado de cliente a varios dispositivos
Uso de SCEP para enviar certificados de cliente a los dispositivos

Creación de un perfil de registro único

Se admiten perfiles de registro único para dispositivos con BlackBerry 10 e iOS. Para configurar la autenticación de registro único para aplicaciones de BlackBerry Dynamics, consulte Configuración de Kerberos para aplicaciones de BlackBerry Dynamics

Antes de empezar:

- Si desea configurar la autenticación de Kerberos en los dispositivos con BlackBerry 10, busque el archivo de configuración de la empresa de Kerberos (krb5.conf).
- Si desea utilizar la autenticación basada en certificados de los dispositivos que ejecutan iOS 8.0 y posteriores, cree el perfil de certificado compartido necesario o el perfil SCEP.

1. En la barra de menú, haga clic en **Políticas y perfiles**.
2. Haga clic en **Redes y conexiones > Registro único**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil.
5. Lleve a cabo cualquiera de las tareas siguientes:

Tarea	Pasos
Configuración de la autenticación de Kerberos de los dispositivos iOS	**a.** Haga clic en la pestaña **iOS**. **b.** En **Kerberos**, haga clic en +. **c.** En el campo **Nombre**, escriba un nombre para la configuración. **d.** En el campo **Nombre principal**, escriba el nombre de Kerberos principal con el formato <*principal*>/<*instancia*>@<*dominio*> (por ejemplo, `user/admin@blackberry.example.com`). **e.** En el campo **Alcance**, escriba el alcance de Kerberos en mayúsculas (por ejemplo, **EXAMPLE.COM**). **f.** En el campo **Prefijos de URL**, escriba el prefijo de la URL de los sitios web con los que desea que los dispositivos se autentiquen. El prefijo debe comenzar con http:// o https:// y pueden incluir valores comodín (*) (por ejemplo, **https://www.blackberry.example.com/***). **g.** Para especificar más prefijos de URL, haga clic en + para agregar más campos. **h.** Si desea limitar la configuración a aplicaciones específicas, haga clic en + al lado de **Identificadores de aplicación**. Escriba el ID de paquete de aplicación. Puede utilizar un valor comodín (*) para que hacer que el ID coincida con varias aplicaciones. (Por ejemplo, **com.company.***). **i.** Para especificar más identificadores de aplicación, haga clic en + para agregar más campos. **j.** Si desea que los dispositivos que ejecutan iOS 8.0 y posteriores utilicen la autenticación basada en certificados, en la lista desplegable **Credenciales**, haga clic en **Certificado**, **SCEP** o **Credenciales del usuario**. En la lista desplegable de certificados, haga clic en el perfil de certificado que desee utilizar. **k.** Haga clic en **Agregar**. **l.** Si fuera necesario, repita los pasos 2 a 11 para agregar otra configuración de Kerberos.
Configuración de la autenticación de Kerberos de los dispositivos BlackBerry 10	**a.** Haga clic en la pestaña **BlackBerry**. **b.** Haga clic en **Examinar**. Navegue y seleccione el archivo de configuración de la empresa de Kerberos (krb5.conf).

Tarea	Pasos
Configuración de la autenticación NTLM o los dominios de confianza de certificados SCEP en los dispositivos con BlackBerry 10	**a.** Haga clic en la pestaña **BlackBerry**. **b.** En **Dominios de confianza**, haga clic en +. **c.** En el campo **Nombre**, escriba un nombre para la configuración. **d.** En el campo **Dominio**, escriba un subdominio de confianza o host individual donde las credenciales de dominio se puedan utilizar para autenticarse automáticamente. Escriba el nombre del servidor como FQDN, nombre de host, alias o dirección IP. Los nombres DNS pueden contener comodines (*). **e.** Para especificar más subdominios, haga clic en + para agregar más campos. **f.** Haga clic en **Agregar**. **g.** Si fuera necesario, repita los pasos 2 a 6 para agregar otro dominio de confianza.

6. Haga clic en **Agregar**.

Después de terminar: Si fuera necesario, clasifique los perfiles.

Conceptos relacionados

Envío del mismo certificado de cliente a varios dispositivos
Uso de SCEP para enviar certificados de cliente a los dispositivos

Tareas relacionadas

Asignación de un perfil o una política de TI a un grupo de usuarios
Asignar un perfil o una política de TI a una cuenta de usuario

Filtrado de contenido web en los dispositivos iOS

Puede utilizar perfiles de filtro de contenido web para limitar los sitios web que un usuario puede ver en Safari o en otras aplicaciones de navegador en un dispositivo iOS. Se pueden asignar perfiles de filtro de contenido web a cuentas de usuarios, a grupos de usuarios y a grupos de dispositivos.

Al crear un perfil de filtro de contenido web, podrá elegir la opción de sitios web permitidos que admite los estándares de la empresa para el uso de dispositivos móviles.

Nota: Este perfil se aplica únicamente a dispositivos iOS supervisados.

Sitios web permitidos	Descripción
Solo sitios web específicos	En esta opción se permite solo el acceso a los sitios web que se especifiquen. Se crea un marcador en Safari para cada sitio web permitido.

Sitios web permitidos	Descripción
Limitar contenido para adultos	Esta opción activa el filtrado automático para identificar y bloquear contenido inapropiado. También puede incluir sitios web específicos utilizando los siguientes ajustes: • URL permitidas: puede agregar una o más direcciones URL para permitir el acceso a sitios web específicos. Los usuarios pueden ver sitios web de esta lista, independientemente de si el filtrado automático bloquea el acceso. • URL en la lista negra: puede agregar una o más direcciones URL para permitir el acceso a sitios web específicos. Los usuarios no pueden ver sitios web de esta lista, independientemente de si el filtrado automático permite el acceso.

Creación de un perfil de filtro de contenido web

Cuando se crea un perfil de filtro de contenido web, cada una de las URL que especifique debe comenzar con http:// o https://. Si es necesario, debe agregar entradas separadas para las versiones http:// o https:// de la misma URL. La resolución de DNS no se produce, por lo tanto, los sitios web de acceso restringido aún podrían ser accesibles (por ejemplo, si especifica http://www.example.com los usuarios pueden acceder a la web utilizando la dirección IP).

1. En la barra de menú, haga clic en **Políticas y perfiles**.
2. Haga clic en **Redes y conexiones > Filtro de contenido web**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil de filtro de contenido web.
5. Lleve a cabo una de las tareas siguientes:

Tarea	Pasos
Permitir el acceso solo a sitios web específicos	a. En la lista desplegable **Sitios web permitidos**, compruebe que esté seleccionada la opción **Solo sitios web específicos**. b. En la sección **Sitios web favoritos específicos**, haga clic en +. c. Realice las acciones siguientes: 1. En el campo **URL**, escriba la dirección web para la que desea permitir el acceso. 2. Opcionalmente, en el campo **Ruta de favoritos**, escriba el nombre de una carpeta de favoritos (por ejemplo, /Trabajo/). 3. En el campo **Título**, escriba un nombre para el sitio web. 4. Haga clic en **Agregar**. d. Repetir los pasos 2 y 3 para cada sitio web permitido.

Tarea	Pasos
Limitar contenido para adultos	**a.** En la lista desplegable **Sitios web permitidos**, haga clic en **Limitar contenido para adultos** para activar el filtrado automático. **b.** Opcionalmente, lleve a cabo las acciones siguientes: **1.** Haga clic en + al lado de **URL permitidas**. **2.** Escriba la dirección web para la que desea permitir el acceso. **3.** Repetir los pasos 2.a y 2.b para cada sitio web permitido. **c.** Opcionalmente, lleve a cabo las acciones siguientes: **1.** Haga clic en + al lado de **URL en la lista negra**. **2.** Escriba la dirección web para la que desea denegar el acceso. **3.** Repetir los pasos 3.a y 3.b para cada sitio web restringido.

6. Haga clic en **Agregar**.

Tareas relacionadas

Asignación de un perfil o una política de TI a un grupo de usuarios
Asignar un perfil o una política de TI a una cuenta de usuario

Gestión del correo y de los dominios web para los dispositivos iOS

Puede utilizar un perfil de dominios gestionados para definir determinados dominios de correo y dominios web como "dominios gestionados" que son internos a la empresa. Los perfiles de dominios gestionados solo se aplican a dispositivos con iOS 8 o posterior con el tipo de activación Controles de MDM.

Después de asignar un perfil de dominios gestionados:

- Cuando un usuario crea un mensaje de correo electrónico y agrega una dirección de correo electrónico del destinatario con un dominio que no está especificado en el perfil de dominios gestionados, el dispositivo muestra la dirección en color rojo para advertir al usuario de que el destinatario es externo a la empresa. El dispositivo no impedirá al usuario enviar correo a destinatarios externos.
- Un usuario debe usar una aplicación que se gestione mediante BlackBerry UEM para ver documentos desde un dominio web gestionado o documentos descargados desde un dominio web gestionado. El dispositivo no impide al usuario visitar o ver documentos desde otros dominios web. El perfil de dominios gestionados se aplica solamente al navegador Safari.

Creación de un perfil de dominios gestionados

Los perfiles de dominios gestionados solo se aplican a dispositivos con iOS 8 o posterior con el tipo de activación Controles de MDM.

1. En la barra de menú, haga clic en **Políticas y perfiles**.
2. Haga clic en **Redes y conexiones > Dominios gestionados**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil.
5. Opcionalmente, en el campo **Descripción**, escriba una descripción para el perfil.
6. En la sección **Dominios de correo electrónico gestionados**, haga clic en +.

7. En el campo **Dominios de correo electrónico**, escriba un nombre de dominio de nivel superior (por ejemplo, `ejemplo.com` en lugar de `ejemplo.com/canada`).
8. Haga clic en **Agregar**.
9. En la sección **Dominios web gestionados**, haga clic en +. Para ver ejemplos de formatos de dominio web, consulte Dominios web gestionados de Safari en la biblioteca del desarrollador de iOS.
10. En el campo **Dominios web**, escriba un nombre de dominio.
11. Si desea permitir que se rellene automáticamente la contraseña para los dominios web que ha especificado, seleccione la casilla de verificación **Permitir autorrelleno de la contraseña**. Esta opción solo es compatible con los dispositivos supervisados iOS con iOS 9.3 o posterior.
12. Haga clic en **Agregar**.
13. Haga clic en **Agregar**.

Tareas relacionadas

Asignación de un perfil o una política de TI a un grupo de usuarios
Asignar un perfil o una política de TI a una cuenta de usuario

Creación de un perfil de AirPrint

Puede configurar los perfiles de AirPrint y asignarlos a los dispositivos con iOS 7 o una versión posterior para que los usuarios no tengan que configurar las impresoras manualmente. Los perfiles de AirPrint pueden ayudar a los usuarios a encontrar impresoras que sean compatibles con AirPrint, que les sean accesibles y para las que tengan los permisos necesarios.

1. En la barra de menú, haga clic en **Políticas y perfiles**.
2. Haga clic en **Redes y conexiones > AirPrint**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil de AirPrint.
5. En la sección **Configuración de AirPrint**, haga clic en +.
6. En el campo **Dirección IP**, escriba la dirección IP de la impresora o del servidor de AirPrint.
7. Opcionalmente, en el campo **Ruta del recurso**, escriba la ruta del recurso de la impresora.
   La ruta del recurso de la impresora corresponde al `rp` del registro Bonjour `_ipps.tcp`. Por ejemplo:
   - printers/<*series de impresoras*>
   - printers/<*modelo de impresora*>
   - ipp/print
   - IPP_Printer
8. Haga clic en **Agregar**.
9. Haga clic en **Agregar**.

Tareas relacionadas

Asignación de un perfil o una política de TI a un grupo de usuarios
Asignar un perfil o una política de TI a una cuenta de usuario

Configuración de perfiles de AirPlay para los dispositivos iOS

Puede configurar los perfiles de AirPlay y asignarlos a los dispositivos con iOS 7 o una versión posterior. AirPlay es una función de iOS que permite mostrar fotos o transmitir música y vídeo a dispositivos AirPlay compatibles, tales como TV Apple, AirPort Express, o altavoces activados de AirPlay.

Con un perfil de AirPlay se pueden establecer contraseñas de dispositivos AirPlay específicos que aseguren que solo los usuarios autorizados puedan acceder a ellos. También se puede crear una lista de dispositivos de destino permitidos que aseguren que los dispositivos iOS supervisados se puedan conectar únicamente con los dispositivos AirPlay que especifique. Se pueden asignar perfiles de AirPlay a cuentas de usuarios, a grupos de usuarios y a grupos de dispositivos.

Ejemplo: Establezca una contraseña para el dispositivo AirPlay

Si desea restringir el acceso a un dispositivo AirPlay específico, agregue el nombre del dispositivo y establezca una contraseña.Los usuarios de dispositivos iOS con ese perfil de AirPlay tendrán que escribir la contraseña para acceder a dicho dispositivo AirPlay. Tenga en cuenta que el perfil de AirPlay requiere la contraseña, no el propio dispositivo AirPlay.Los usuarios de los dispositivos iOS que no tienen ese perfil de AirPlay todavía pueden acceder al dispositivo AirPlay sin la contraseña.

Ejemplo: Cree una lista de dispositivos AirPlay para los dispositivos iOS supervisados

Si desea permitir que los dispositivos iOS supervisados transmitan contenido solo para dispositivos específicos, puede agregar el ID del dispositivo. Los dispositivos supervisados solo podrán transmitir contenidos a los dispositivos que se especifiquen. Los dispositivos que no están supervisados no se verán afectados por esta lista.

Creación de un perfil de AirPlay

1. En la barra de menú, haga clic en **Políticas y perfiles**.
2. Haga clic en **Redes y conexiones > AirPlay**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil de AirPlay.
5. Haga clic en + en la sección **Dispositivos de destino permitidos**.
6. En el campo **Nombre del dispositivo**, escriba el nombre del dispositivo AirPlay que desea agregar. Puede encontrar el nombre del dispositivo AirPlay en los ajustes del dispositivo o puede buscar el nombre del dispositivo tocando **AirPlay** en el Centro de Control de un dispositivo iOS para ver una lista de dispositivos AirPlay disponibles cerca.
7. En el campo **Contraseña**, escriba la contraseña correcta.
8. Haga clic en **Agregar**.
9. Haga clic en + en la sección **Dispositivos de destino permitidos para los dispositivos supervisados**.
10. En el campo **ID del dispositivo**, escriba el ID de dispositivo AirPlay que desea agregar. Puede encontrar el ID del dispositivo AirPlay en los ajustes del dispositivo. Para obtener más información acerca de cómo buscar el ID de dispositivo, consulte la documentación del producto Apple.
11. Haga clic en **Agregar**.

Tareas relacionadas

Asignación de un perfil o una política de TI a un grupo de usuarios

Asignar un perfil o una política de TI a una cuenta de usuario

Control del uso de la red de las aplicaciones de trabajo en los dispositivos iOS

Puede utilizar un perfil de uso de la red para controlar cómo utilizan la red móvil las aplicaciones de trabajo en los dispositivos que ejecutan iOS 9 o versiones posteriores.

Para administrar el uso de la red, puede evitar que las aplicaciones transfieran datos cuando los dispositivos están conectados a la red móvil o cuando los dispositivos están en roaming. Puede especificar las mismas reglas de uso de red para todas las aplicaciones de trabajo o puede especificar reglas para algunas aplicaciones de trabajo. Un perfil de uso de red puede contener reglas para una aplicación o para varias aplicaciones. Si no se especifican aplicaciones en el perfil, las reglas se aplican a todas las aplicaciones de trabajo.

Creación de un perfil de uso de red

Las reglas de un perfil de uso de la red se aplican únicamente a aplicaciones de trabajo. Si no se han asignado las aplicaciones a los usuarios o a los grupos de usuarios, el perfil de uso de la red no tiene ningún efecto.

Antes de empezar: Agregue aplicaciones a la lista de aplicaciones y asígnelas a los grupos de usuarios o a las cuentas de usuario.

1. En la barra de menú, haga clic en **Políticas y perfiles**.
2. Haga clic en **Redes y conexiones > Uso de red**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil.
5. Haga clic en +.
6. Lleve a cabo una de las siguientes acciones:
   - Toque **Agregar una aplicación** y haga clic en una aplicación de la lista.
   - Seleccione **Especificar el ID de paquete de aplicación** y escriba el ID. El ID de paquete de aplicación también se conoce como ID de paquete. Puede encontrar el ID del paquete de aplicación haciendo clic en la aplicación que se encuentra en la lista de aplicaciones. Utilice un valor comodín (*) para que coincida con el ID de varias aplicaciones. (Por ejemplo, **com.company.***).
7. Para evitar que la aplicación o las aplicaciones utilicen datos cuando el dispositivo está en roaming, desactive la casilla de verificación **Permitir roaming de datos**.
8. Para evitar que la aplicación o las aplicaciones utilicen datos cuando el dispositivo está conectado a la red móvil, desactive la casilla de verificación **Permitir datos móviles**.
9. Haga clic en **Agregar**.
10. Repita los pasos 5 a 8 para cada aplicación que desee agregar a la lista.

Después de terminar: Si fuera necesario, clasifique los perfiles.

Tareas relacionadas

Asignación de un perfil o una política de TI a un grupo de usuarios
Asignar un perfil o una política de TI a una cuenta de usuario

Correo, calendario y contactos

Puede utilizar perfiles para gestionar la forma en la que los dispositivos reciben los mensajes de correo de trabajo, los datos del calendario o la información de los contactos. Puede especificar la configuración de los dispositivos con BlackBerry 10, iOS, macOS, Android y Windows en el mismo perfil y, a continuación, asignar el perfil a las cuentas de usuarios, a los grupos de usuarios o a los grupos de dispositivos.

Si su empresa utiliza BlackBerry Work para gestionar el correo, el calendario y los contactos para los dispositivos de usuarios, puede configurar la aplicación BlackBerry Work en lugar del perfil de correo. Para obtener más información acerca de la gestión de BlackBerry Work, consulte Gestión de aplicaciones de BlackBerry Dynamics y la BlackBerry Work Guía de administración.

Configuración del correo de trabajo para dispositivos

Puede utilizar los perfiles de correo electrónico para especificar cómo se conectan los dispositivos al servidor de correo de la empresa y cómo sincronizan los mensajes de correo, las entradas del calendario y los datos del organizador mediante Exchange ActiveSync o IBM Notes Traveler.

Si desea utilizar Exchange ActiveSync, debe tener en cuenta lo siguiente:

- Para ampliar la seguridad de correo, puede activar S/MIME para dispositivos iOS y dispositivos Android. Puede activar S/MIME o PGP para dispositivos con BlackBerry 10. PGP es compatible con BlackBerry 10 OS versión 10.3.1 o posterior.
- Si activa S/MIME, puede utilizar otros perfiles para permitir que los dispositivos puedan recuperar automáticamente los certificados S/MIME y comprobar el estado del certificado.

Si desea utilizar Notes Traveler, debe tener en cuenta lo siguiente:

- Para utilizar Notes Traveler con dispositivos iOS, debe activar BlackBerry Secure Gateway.
- La sincronización de datos de tareas pendientes solo es compatible con los dispositivos con BlackBerry 10. Utiliza el protocolo de comunicación de SyncML en el servidor Notes Traveler.
- Para ampliar la seguridad de correo en los dispositivos con BlackBerry 10, solo se admite el cifrado de IBM Notes (S/MIME no es compatible).
- Para utilizar Notes Traveler con la aplicación cliente IBM Verse:
  - Para dispositivos con Samsung KNOX, configure los ajustes de IBM Verse en el perfil de correo.
  - para los dispositivos Android que tienen un perfil de trabajo, puede configurar los ajustes de IBM Verse mediante la configuración de aplicación

También puede utilizar perfiles de correo IMAP/POP3 para especificar cómo desea que los dispositivos iOS, macOS, Android y Windows se conecten a los servidores de correo IMAP o POP3 y sincronicen los mensajes de correo. Los dispositivos activados para utilizar KNOX MDM no admiten IMAP ni POP3.

Puede utilizar BlackBerry Work en lugar de un perfil de correo para gestionar el correo, el calendario y los contactos de dispositivos de usuarios. Para obtener más información acerca de la gestión de BlackBerry Work, consulte Gestión de aplicaciones de BlackBerry Dynamics y la BlackBerry Work Guía de administración.

Crear un perfil de correo electrónico

La configuración del perfil obligatorio varía para cada tipo de dispositivo y depende del servidor de correo utilizado en el entorno de la empresa.

Antes de empezar:

- Si utiliza autenticación basada en certificados entre los dispositivos y el servidor de correo, debe crear un perfil de certificado de CA y asignarlo a los usuarios. También se debe asegurar de que los dispositivos tengan un certificado de cliente de confianza.
- Para aplicar automáticamente un perfil de correo a los dispositivos Android, el dispositivo debe cumplir uno de los criterios siguientes. Si el dispositivo no cumple ninguno de estos criterios, BlackBerry UEM envía el perfil de correo a los dispositivos Android, pero el usuario debe configurar manualmente la conexión con el servidor de correo:
  - Dispositivos Android con un perfil de trabajo
  - Dispositivos Samsung KNOX y Samsung KNOX Workspace
  - Dispositivos Motorola
- Si planea utilizar BlackBerry Secure Gateway para proporcionar una conexión segura al servidor de correo de su empresa a través de BlackBerry Infrastructure y BlackBerry UEM para los dispositivos iOS con el tipo de activación Controles de MDM, compruebe que su empresa cuenta con las licencias de BlackBerry UEM adecuadas. Para obtener más información, consulte el contenido referente a Licencias.

1. En la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Correo, Calendario y contactos > Correo**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil.
5. Si fuera necesario, escriba el nombre de dominio del servidor de correo. Si el perfil es para varios usuarios que pueden estar en diferentes dominios de Microsoft Active Directory, puede utilizar la variable `%UserDomain%`.
6. En el campo **Dirección de correo**, realice una de las siguientes acciones:
   - Si el perfil es para un usuario, escriba la dirección de correo del usuario.
   - Si el perfil es para varios usuarios, escriba `%UserEmailAddress%`.
7. Escriba el nombre de host o la dirección IP del servidor de correo.
8. En el campo **Nombre de usuario**, realice una de las siguientes acciones:
   - Si el perfil es para un usuario, escriba el nombre de usuario.
   - Si el perfil es para varios usuarios, escriba `%UserName%`.
   - Si el perfil es para varios usuarios en un entorno IBM Notes Traveler, escriba `%UserDisplayName%`.
9. Si ha configurado grupos de servidores para dirigir el tráfico de BlackBerry Secure Gateway o el tráfico de BlackBerry Gatekeeping Service a una conexión regional determinada de BlackBerry Infrastructure, en la lista desplegable **Grupo de servidores de BlackBerry Secure Gateway Service**, haga clic en el grupo de servidores adecuado.

   Para obtener más información acerca de BlackBerry Connectivity Node y los grupos de servidores, consulte el contenido de Planificación y el contenido de Instalación y actualización.
10. Haga clic en la pestaña para cada tipo de dispositivo en la empresa y configure los valores apropiados para cada configuración de perfil. Para obtener más información acerca de la configuración de cada perfil, consulte Configuración del perfil de correo.
11. Haga clic en **Agregar**.

Después de terminar: Si fuera necesario, clasifique los perfiles.

Conceptos relacionados

Configuración del perfil de correo
Envío de certificados a dispositivos mediante perfiles

Tareas relacionadas

Asignación de un perfil o una política de TI a un grupo de usuarios
Asignar un perfil o una política de TI a una cuenta de usuario

Creación de un perfil de correo IMAP/POP3

La configuración del perfil obligatorio varía para cada tipo de dispositivo y depende de los ajustes que seleccione.

Nota: BlackBerry UEM envía el perfil de correo a los dispositivos Android, pero el usuario debe configurar manualmente la conexión con el servidor de correo.

1. En la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Correo, Calendario y contactos > Correo IMAP/POP3**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil.
5. En el campo **Tipo de correo**, seleccione el tipo de protocolo de correo.
6. En el campo **Dirección de correo**, realice una de las siguientes acciones:
   - Si el perfil es para un usuario, escriba la dirección de correo del usuario.
   - Si el perfil es para varios usuarios, escriba `%UserEmailAddress%`.
7. En la sección **Configuración del correo electrónico entrante**, escriba el nombre de host o la dirección IP del servidor de correo para recibir el correo.
8. Si fuera necesario, escriba el puerto para recibir correo.
9. En el campo **Nombre de usuario**, realice una de las siguientes acciones:
   - Si el perfil es para un usuario, escriba el nombre de usuario.
   - Si el perfil es para varios usuarios, escriba `%UserName%`.
10. En la sección **Configuración del correo saliente**, escriba el nombre de host o la dirección IP del servidor de correo para enviar correo.
11. Si fuera necesario, escriba el puerto para enviar correo.
12. Si fuera necesario, seleccione **Autenticación requerida para el correo de salida** y especifique las credenciales utilizadas para enviar correo.
13. Haga clic en la pestaña para cada tipo de dispositivo en la empresa y configure los valores apropiados para cada configuración de perfil. Para obtener más información acerca de la configuración de cada perfil, consulte Configuración del perfil de correo IMAP/POP3.
14. Haga clic en **Agregar**.

Conceptos relacionados

Configuración del perfil de correo IMAP/POP3

Tareas relacionadas

Asignación de un perfil o una política de TI a un grupo de usuarios
Asignar un perfil o una política de TI a una cuenta de usuario

Protección de datos de correo electrónico mediante BlackBerry Secure Gateway

BlackBerry Secure Gateway proporciona una conexión segura a través de BlackBerry Infrastructure y BlackBerry UEM al servidor de correo de su empresa para dispositivos iOS que están activados con Controles de MDM.

La activación de BlackBerry Secure Gateway permite que los dispositivos que están activados con Controles de MDM envíen y reciban correo de trabajo sin tener que exponer su servidor de correo fuera del firewall o ubicar el servidor de correo en una DMZ.

Si planea utilizar BlackBerry Secure Gateway, debe verificar que su empresa cuente con las licencias de BlackBerry UEM correspondientes. Para obtener más información, consulte el contenido referente a Licencias.

Para activar BlackBerry Secure Gateway, seleccione la configuración "Activar BlackBerry Secure Gateway " en el perfil de correo.

Si ha configurado grupos de servidores para admitir conexiones regionales con BlackBerry Infrastructure, puede dirigir el tráfico de BlackBerry Secure Gateway a una conexión regional específica mediante la asociación del perfil de correo electrónico con el grupo de servidores apropiado.

Ampliación de la seguridad del correo mediante S/MIME

Puede ampliar la seguridad del correo para los usuarios de dispositivos con BlackBerry 10, iOS y Android al activar S/MIME. S/MIME proporciona un método estándar para cifrar y firmar mensajes de correo. Los usuarios pueden cifrar, firmar o cifrar y firmar mensajes de correo utilizando la protección S/MIME cuando utilizan una cuenta de correo de trabajo que admita mensajes protegidos con S/MIME en los dispositivos. S/MIME no se puede activar para las direcciones de correo personales.

Los usuarios pueden guardar los certificados S/MIME del destinatario en sus dispositivos. Los usuarios pueden almacenar sus claves privadas en sus dispositivos o en una tarjeta inteligente.

Active S/MIME para los usuarios en un perfil de correo. Puede forzar a los usuarios del dispositivo con BlackBerry 10 a utilizar S/MIME, pero no a los usuarios del dispositivo iOS o Android. Cuando el uso de S/MIME es opcional, un usuario puede activar S/MIME en el dispositivo y especificar si desea cifrar, firmar o cifrar y firmar mensajes de correo.

La configuración S/MIME tiene prioridad sobre la configuración de PGP. Cuando la compatibilidad de S/MIME se establece en "Obligatorio", los ajustes de PGP se ignoran.

Recuperación de certificados S/MIME

Puede utilizar perfiles de recuperación de certificados que permitan a los dispositivos buscar y recuperar los certificados S/MIME de los destinatarios desde los servidores de certificados LDAP. Si el certificado S/MIME todavía no está en el almacén de certificados del dispositivo, el dispositivo lo recupera y lo importa automáticamente al almacén de certificados.

Tipo de dispositivo	Descripción
BlackBerry 10	Los dispositivos buscan cada servidor de certificados LDAP que se especifique en el perfil y recuperan el certificado S/MIME. Si hay más de un certificado S/MIME y un dispositivo no puede determinar el preferido, el dispositivo muestra todos los certificados S/MIME para que el usuario pueda seleccionar el que desea utilizar. Puede solicitar que los dispositivos utilicen tanto la autenticación simple como la autentificación Kerberos con los servidores de certificados LDAP. Si solicita que los dispositivos utilicen la autenticación simple, puede incluir las credenciales de autenticación necesarias en los perfiles de recuperación de certificado de modo que los dispositivos puedan autenticarse automáticamente con los servidores de certificados LDAP. Si solicita que los dispositivos utilicen la autenticación Kerberos, puede incluir las credenciales de autenticación necesarias en los perfiles de recuperación de certificado de forma que los dispositivos que ejecutan la versión 10.3.1 de BlackBerry 10 OS y posteriores puedan autenticarse automáticamente con los servidores de certificado LDAP. De lo contrario, el dispositivo solicitará al usuario las credenciales de autenticación necesarias la primera vez que el dispositivo intente autenticarse en un servidor de certificados LDAP. Para dispositivos que ejecutan BlackBerry 10 OS de la versión 10.2.1 a la 10.3, el dispositivo solicitará al usuario las credenciales de autenticación necesarias la primera vez que el dispositivo intente autenticarse en un servidor de certificados LDAP. Si implementa la autenticación Kerberos para la recuperación de certificados S/MIME, debe asignar un perfil de inicio de sesión único aplicable a los usuarios o grupos de usuarios aplicables. Para obtener más información acerca de cómo crear y asignar un perfil de inicio de sesión único, consulte Configuración de la autenticación de registro único de los dispositivos.

Si no crea un perfil de recuperación de certificados y lo asigna a cuentas de usuario, a grupos de usuarios o a grupos de dispositivos, los usuarios deberán importar manualmente los certificados S/MIME desde un archivo adjunto al correo de trabajo o desde un equipo.

Creación de un perfil de recuperación de certificados

Antes de empezar:

- Para permitir que los dispositivos puedan confiar en los servidores de certificados LDAP cuando hacen conexiones seguras, puede que necesite distribuir certificados de CA en los dispositivos. Si es necesario, cree los perfiles de certificado de CA y asígnelos a las cuentas de usuarios, a los grupos de usuarios o a los grupos de dispositivos. Para obtener más información acerca de los certificados de CA, consulte Envío de certificados de CA a los dispositivos.
- Si implementa la autenticación Kerberos para la recuperación de certificados S/MIME, debe asignar un perfil de inicio de sesión único aplicable a los usuarios o grupos de usuarios aplicables. Para obtener más información acerca de los perfiles de inicio de sesión único, consulte Configuración de la autenticación de registro único de los dispositivos.

1. En la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Certificados > Recuperación de certificado**.
3. Haga clic en +.

4. Escriba un nombre y una descripción para el perfil de recuperación de certificados.
5. En la tabla, haga clic en +.
6. En el campo **URL de servicio**, escriba el servidor de certificados FQDN o LDAP con el formato ldap://<*fqdn*>:<*puerto*>. (Por ejemplo, ldap://server01.example.com:389).
7. En el campo **Base de búsqueda**, escriba el DN de base que sea el punto de partida para las búsquedas del servidor de certificados LDAP.
8. En la lista desplegable **Ámbito de búsqueda**, lleve a cabo una de las siguientes acciones:
   - Para buscar solo el objeto base (DN de base), haga clic en **Base**. Esta opción es el valor predeterminado.
   - Para buscar en un nivel por debajo del objeto base, pero no el objeto base, haga clic en **Un nivel**.
   - Para buscar el objeto base y todos los niveles por debajo, haga clic en **Subárbol**.
   - Para buscar en todos los niveles por debajo del objeto base, pero no el objeto base, haga clic en **Secundario**.
9. Si se necesita autenticación, realice las acciones siguientes:
   a) En la lista desplegable **Tipo de autenticación**, haga clic en **Simple** o en **Kerberos**.
   b) En el campo **ID de usuario de LDAP**, escriba el DN de una cuenta que disponga de permisos de búsqueda en el servidor de certificados LDAP (por ejemplo, cn=admin,dc=ejemplo,dc=com).
   c) En el campo **Contraseña de LDAP**, escriba la contraseña de la cuenta que tenga permisos de búsqueda en el servidor de certificados LDAP.
10. Si fuera necesario, seleccione la casilla de verificación **Usar conexión segura**.
11. En el campo **Tiempo de espera de conexión**, escriba la cantidad de tiempo, en segundos, que el dispositivo espera la respuesta del servidor de certificados LDAP.
12. Haga clic en **Agregar**.
13. Repita los pasos del 5 al 11 para cada servidor de certificados LDAP.
14. Haga clic en **Agregar**.

Después de terminar:

- Para permitir que los dispositivos con BlackBerry 10 comprueben el estado del certificado, cree un perfil OCSP o CRL.
- Si fuera necesario, clasifique los perfiles.

Tareas relacionadas

Creación de un perfil OCSP
Creación de un perfil CRL
Asignación de un perfil o una política de TI a un grupo de usuarios
Asignar un perfil o una política de TI a una cuenta de usuario

Determinación del estado de los certificados S/MIME en dispositivos

Puede utilizar perfiles CRL y OCSP para permitir que los dispositivos con BlackBerry 10 comprueben el estado de los certificados S/MIME. Se puede asignar un perfil OCSP y uno CRL a cuentas de usuarios, a grupos de usuarios y a grupos de dispositivos.

Los dispositivos con BlackBerry 10 buscan cada respondedor OCSP que especifica en un perfil OCSP y recuperan el estado del certificado S/MIME. Los dispositivos que ejecutan la versión 10.3.1 de BlackBerry 10 OS y posteriores pueden enviar solicitudes de estado de certificado a BlackBerry UEM, y puede utilizar perfiles CRL para configurar BlackBerry UEM para buscar el estado de los certificados S/MIME mediante HTTP, HTTPS o LDAP.

Si se utiliza Exchange ActiveSync para la recuperación del certificado, los dispositivos iOS y Android utilizarán Exchange ActiveSync para verificar el estado de los certificados S/MIME. Si se utiliza LDAP para la recuperación del certificado, los dispositivos iOS y Android utilizarán OCSP para verificar el estado de los certificados.Los dispositivos iOS y Android no utilizan perfiles OCSP. Los dispositivos verifican el respondedor OCSP con el certificado.

Para obtener más información sobre los indicadores de estado del certificado, consulte la guía de usuario del dispositivo para conocer los detalles acerca de los iconos de correo electrónico seguros.

Creación de un perfil OCSP

Los perfiles OCSP son compatibles con los dispositivos BlackBerry 10.

1. En la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Certificados > OCSP**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil OCSP.
5. Realice las acciones siguientes:
   a) En la tabla, haga clic en +.
   b) En el campo **URL de servicio**, escriba la dirección web de un respondedor OCSP.
   c) En el campo **Tiempo de espera de conexión**, escriba la cantidad de tiempo, en segundos, que el dispositivo espera la respuesta de OCSP.
   d) Haga clic en **Agregar**.
6. Repita el paso 4 para cada respondedor OCSP.
7. Haga clic en **Agregar**.

Después de terminar: Si fuera necesario, clasifique los perfiles.

Tareas relacionadas

Asignación de un perfil o una política de TI a un grupo de usuarios
Asignar un perfil o una política de TI a una cuenta de usuario

Creación de un perfil CRL

Los perfiles CRL son compatibles con los dispositivos BlackBerry 10 y BlackBerry con Android con Android 7.0 y posterior.

1. En la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Certificados > CRL**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil CRL.
5. Para permitir que los dispositivos puedan utilizar las URL de respondedor definidas en el certificado, seleccione la casilla de verificación **Usar respondedores de extensión de certificado**.
6. Lleve a cabo cualquiera de las tareas siguientes:

Tarea	Pasos
Especificación de la configuración CRL de HTTP	**a.** En la sección **HTTP para CRL**, haga clic en +. **b.** Escriba un nombre y una descripción para la configuración CRL de HTTP. **c.** En el campo **URL de servicio**, escriba la dirección web de un servidor HTTP o HTTPS. **d.** Haga clic en **Agregar**. **e.** Repita los pasos del 1 al 4 para cada servidor HTTP o HTTPS.
Especificación de la configuración CRL de LDAP	**a.** En la sección **LDAP para CRL**, haga clic en +. **b.** Escriba un nombre y una descripción para la configuración CRL de LDAP. **c.** En el campo **URL de servicio**, escriba el servidor FQDN o LDAP con el formato ldap://<*fqdn*>:<*port*> (por ejemplo, ldap://server01.example.com:389). Para conexiones seguras, utilice el formato ldaps://<*fqdn*>:<*port*>. **d.** En el campo **Base de búsqueda**, escriba el DN de base que sea el punto de partida para las búsquedas del servidor LDAP. **e.** Si fuera necesario, seleccione la casilla de verificación **Usar conexión segura**. **f.** En el campo **ID de usuario de LDAP**, escriba el DN de una cuenta que disponga de permisos de búsqueda en el servidor LDAP (por ejemplo, cn=admin,dc=ejemplo,dc=com). **g.** En el campo **Contraseña de LDAP**, escriba la contraseña de la cuenta que tenga permisos de búsqueda en el servidor LDAP. **h.** Haga clic en **Agregar**. **i.** Repita los pasos del 1 al 8 para cada servidor LDAP.

7. Haga clic en **Agregar**.

Después de terminar: Si fuera necesario, clasifique los perfiles.

Tareas relacionadas

Asignación de un perfil o una política de TI a un grupo de usuarios
Asignar un perfil o una política de TI a una cuenta de usuario

Ampliación de la seguridad del correo mediante PGP

Para los dispositivos que ejecutan la versión BlackBerry 10 OS 10.3.1 y posteriores, puede ampliar la seguridad del correo para los usuarios de los dispositivos mediante la activación de PGP. PGP protege los mensajes de correo en dispositivos mediante el formato OpenPGP. Los usuarios pueden firmar, cifrar o firmar y cifrar mensajes de correo con la protección PGP al utilizar una dirección de correo de trabajo. PGP no se puede activar para las direcciones de correo personales.

Active PGP para los usuarios en un perfil de correo. Puede forzar a los usuarios del dispositivo con BlackBerry 10 a utilizar PGP, no permitir el uso de PGP o hacerlo opcional. Cuando el uso de PGP es opcional (el valor predeterminado), un usuario puede activar PGP en el dispositivo y especificar si desea cifrar, firmar o cifrar y firmar mensajes de correo.

Para firmar y cifrar mensajes de correo, los usuarios deben guardar claves PGP para cada destinatario en sus dispositivos. Los usuarios pueden guardar claves PGP importando los archivos desde un mensaje de correo de trabajo.

Puede configurar PGP mediante las configuraciones del perfil de correo adecuadas.

Referencia relacionada

BlackBerry 10: ajustes del perfil de correo

Aplicación de un correo protegido mediante la clasificación de mensajes

La clasificación de mensajes permite a la empresa especificar e imponer políticas de correo electrónico seguras y agregar marcas visuales a los mensajes de correo electrónico en los dispositivos con BlackBerry 10. Puede utilizar BlackBerry UEM para proporcionar a los usuarios de dispositivos con BlackBerry 10 opciones de clasificación de mensajes similares a las que están disponibles en las aplicaciones de correo electrónico de su ordenador. Puede definir las siguientes reglas a aplicar a los mensajes salientes, en función de las clasificaciones de los mensajes:

- Agregar una etiqueta para identificar la clasificación de mensajes (por ejemplo, Confidencial)
- Agregar un marcador visual al final de la línea del asunto (por ejemplo, [C])
- Agregar texto al principio o al final del cuerpo de un mensaje de correo electrónico (por ejemplo, "Este mensaje ha sido clasificado como confidencial")
- Configurar S/MIME o las opciones de PGP (por ejemplo, firmar y cifrar)
- Configurar una clasificación predeterminada

Para los dispositivos que ejecutan BlackBerry 10 OS versión 10.3.1 y posterior, puede utilizar la clasificación de mensajes para solicitar a los usuarios que firmen, cifren o que firmen y cifren los mensajes de correo electrónico, así como para agregar marcas visuales a los mensajes de correo electrónico que envían desde sus dispositivos. Puede utilizar perfiles de correo para especificar la configuración de clasificación de mensajes (con extensiones de nombre de archivo .json) para enviar a los dispositivos de los usuarios. Cuando los usuarios responden a los mensajes de correo que tienen la clasificación de mensajes configurada o bien redacta los mensajes de correo protegido, la configuración de la clasificación de mensajes determina las reglas de clasificación que los dispositivos deben aplicar al mensaje saliente.

Las opciones de protección de mensajes en un dispositivo se limitan a los tipos de cifrado y firma digital que se permiten en el dispositivo. Cuando un usuario aplica una clasificación de mensajes a un mensaje de correo electrónico en el dispositivo, el usuario debe seleccionar uno de los tipos de protección de mensajes que permite dicha clasificación o aceptar el tipo de protección de mensajes predeterminado. Si un usuario selecciona una clasificación de mensajes que requiere la firma, el cifrado, o la firma y el cifrado del mensaje, y si el dispositivo no tiene configurado S/MIME o PGP, el usuario no puede enviar el mensaje de correo electrónico.

Los ajustes de S/MIME y de PGP tienen prioridad sobre los mensajes de clasificación. Los usuarios pueden aumentar, pero no reducir, los niveles de clasificación de los mensajes en sus dispositivos. Los niveles de clasificación de los mensajes están determinados por las reglas de correo electrónico seguro de cada clasificación.

Cuando la clasificación de mensajes está activada, los usuarios no pueden utilizar BlackBerry Assistant para enviar mensajes de correo desde los dispositivos.

Puede configurar la clasificación de mensajes mediante las adecuadas configuraciones del perfil de correo.

Para obtener más información acerca de cómo crear archivos de configuración de clasificación de mensajes, visite support.blackberry.com/kb y lea el artículo KB36736.

Referencia relacionada

BlackBerry 10: ajustes del perfil de correo

Configuración de dominios permitidos y restringidos en dispositivos con un espacio de trabajo

Para prevenir la fuga de datos, puede configurar los dominios a los que pueden acceder los usuarios desde el correo, el calendario y los datos del organizador en el espacio de trabajo en los dispositivos iOS y Android.

- Si configura una lista de dominios permitidos, los usuarios pueden tener acceso a dominios permitidos sin restricciones. Por ejemplo, pueden hacer clic en los vínculos al dominio o agregar destinatarios con direcciones de correo electrónico en el dominio para enviar mensajes de correo o invitaciones de calendario. Si un dominio particular no está en la lista de permitidos, la aplicación muestra un mensaje de advertencia cuando un usuario intenta acceder a él. Si el usuario toca Aceptar, puede acceder al dominio.
- Si configura una lista restringida de los dominios, los usuarios no pueden acceder a ninguno de los dominios que figuren en la lista. Si hacen clic en los vínculos al dominio o intentan agregar destinatarios con direcciones de correo electrónico en el dominio, la aplicación presenta un mensaje de error y no permite que el usuario complete la tarea. Un usuario puede acceder a los dominios que no estén en la lista de restringidos.

Nota: Para dispositivos con BlackBerry 10, puede configurar dominios permitidos y restringidos utilizando las reglas de políticas de TI "Lista de dominios de correo externos permitidos" y "Lista de dominios de correo externos restringidos". Para obtener más información, descargue la hoja de cálculo de referencia de políticas.

Configuración de dominios permitidos y restringidos en el espacio de trabajo

1. En la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Correo, Calendario y contactos > Correo**.
3. Seleccione el perfil de correo que desee cambiar.
4. Haga clic en ✎.
5. Haga clic en la pestaña **iOS** o **Android**.
6. En la sección de **Dominios de correo electrónico externos**, agregue los dominios que desea permitir y los que desea restringir.
7. Haga clic en **Guardar**.

Referencia relacionada

Android: ajustes del perfil de correo
iOS: ajustes del perfil de correo

Uso de Enlace de Exchange

Su empresa puede utilizar el BlackBerry Gatekeeping Service para controlar qué dispositivos pueden acceder a Exchange ActiveSync.

Para usar enlaces en BlackBerry UEM, debe completar las siguientes tareas:

- Cree una configuración de enlace. En el contenido de configuración, consulte Supervisión de los dispositivos que pueden acceder a Exchange ActiveSync.
- Creación de un perfil de enlace

Si la empresa utiliza BlackBerry Gatekeeping Service, cualquier dispositivo que no se encuentre en la lista blanca de Microsoft Exchange será incluido en la lista de dispositivos BlackBerry UEM restringidos de Exchange ActiveSync.

Si agrega una cuenta de usuario y le asigna un perfil de enlace, todos los dispositivos que estaban previamente bloqueados, en cuarentena o permitidos manualmente relacionados con la cuenta de usuario aparecerán en la lista de dispositivos Exchange ActiveSync restringidos.

Permitir que un dispositivo tenga acceso a Microsoft ActiveSync

Si BlackBerry UEM no puede obtener un ID de Exchange ActiveSync de un dispositivo, no se agregará a la lista de permitidos de Microsoft Exchange. Puede agregar manualmente estos dispositivos a la lista de permitidos desde la lista de dispositivos Exchange ActiveSync restringidos. Por ejemplo, si un dispositivo Android se activa con el tipo de activación de MDM, BlackBerry UEM no podrá obtener un ID de Exchange ActiveSync y deberá introducir manualmente el dispositivo en la lista blanca de la lista de dispositivos Exchange ActiveSync restringidos.

1. En la barra de menú, haga clic en **Usuarios > Enlace de Exchange**.
2. Busque un dispositivo.
3. En la columna **Acción**, haga clic en ✓.

Bloqueo de un dispositivo para que no acceda a Microsoft ActiveSync

Puede bloquear manualmente un dispositivo permitido previamente para que no acceda a Microsoft ActiveSync. El bloqueo de un dispositivo evita que un usuario recupere mensajes de correo y otra información de Microsoft Exchange Server del dispositivo.

1. En la barra de menú, haga clic en **Usuarios**.
2. Haga clic en **Enlace de Exchange**.
3. Busque un dispositivo.
4. En la columna **Acción**, haga clic en ⊘.

Comprobación para permitir que un dispositivo tenga acceso al correo de trabajo y a los datos del organizador

Si la empresa utiliza BlackBerry Gatekeeping Service para controlar los dispositivos que pueden acceder al correo de trabajo y a los datos del organizador desde Exchange ActiveSync, al menos un servidor de enlace deberá estar configurado en un perfil de correo. Si el perfil de correo con enlace configurado está asignado a una cuenta de usuario, podrá comprobar el estado de la conexión entre un dispositivo y Exchange ActiveSync. Puede ubicar dicho estado si consulta la página de detalles del dispositivo, en la sección de política de TI y perfiles. Los estados siguientes se muestran en los detalles del dispositivo al lado del perfil de correo.

Estado	Descripción
Desconocido	Aparecerá el estado de desconocido si BlackBerry UEM no puede determinar el ID del dispositivo. El dispositivo aparecerá en la lista de dispositivos restringidos y deberá agregarse manualmente a la lista de permitidos.
Conexión pendiente	Se mostrará un estado de conexión pendiente si BlackBerry UEM conoce el ID del dispositivo y este se ha puesto en cola y está a la espera de ser agregado a la lista de permitidos.
Conexión permitida	Se mostrará un estado de conexión permitida si BlackBerry UEM conoce el ID del dispositivo y este se encuentra en la lista de permitidos.

Comprobación de que el dispositivo esté permitido

1. En la barra de menú, haga clic en **Usuarios > Dispositivos gestionados**.
2. Busque una cuenta de usuario.
3. En los resultados de la búsqueda, haga clic en el nombre de una cuenta de usuario.
4. Seleccione la pestaña del dispositivo que desea comprobar.
5. En la sección **Política de TI y perfiles**, si el dispositivo está permitido, se mostrará **Conexión permitida** al lado del perfil de correo.

Creación de un perfil de enlace

Si ha configurado BlackBerry Gatekeeping Service, debe crear un perfil de enlace y asígnelo a cuentas de usuarios, grupos de usuarios o grupos de dispositivos. El perfil de enlace permite seleccionar los servidores de Microsoft Exchange para el enlace automático.

Creación de un perfil de enlace

Si utiliza un enlace automático, cree un perfil de enlace.

1. En la barra de menú, haga clic en **Policies and Profiles (Políticas y perfiles)**.
2. Haga clic en **Correo, Calendario y contactos > Enlace**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil.
5. Haga clic en **Seleccionar servidores**.
6. Seleccione uno o más servidores y haga clic en →.
7. Haga clic en **Guardar**.

Configuración de los perfiles de CardDAV y CalDAV para los dispositivos iOSy macOS

Puede utilizar perfiles de CardDAV y CalDAV para permitir que los dispositivos iOS y macOS accedan a la información del calendario y a los contactos en un servidor remoto. Se pueden asignar perfiles de CardDAV y CalDAV a cuentas de usuarios, a grupos de usuarios y a grupos de dispositivos. Varios dispositivos pueden acceder a la misma información.

macOS aplica perfiles a las cuentas de usuario o los dispositivos. Los perfiles de CardDAV y CalDAV se aplican a cuentas de usuario.

Creación de un perfil CardDAV

Antes de empezar:

- Compruebe que el dispositivo pueda acceder a un servidor CardDAV activo.

1. En la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Correo, Calendario y contactos > CardDAV**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil.
5. Escriba la dirección del servidor para el perfil. Es el FQDN del equipo que aloja la aplicación Calendario.

6. En el campo **Nombre de usuario**, realice una de las siguientes acciones:
   - Si el perfil es para un usuario, escriba el nombre de usuario.
   - Si el perfil es para varios usuarios, escriba `%UserName%`.
7. Si es necesario, introduzca el puerto para el servidor CardDAV.
8. Si es necesario, seleccione la casilla de verificación **Utilizar SSL** e introduzca la URL para el servidor SSL.
9. Haga clic en **Agregar**.

Después de terminar: Asigne el perfil a los usuarios, a los grupos de usuarios o a los grupos de dispositivos.

Tareas relacionadas

Asignación de un perfil o una política de TI a un grupo de usuarios
Asignar un perfil o una política de TI a una cuenta de usuario

Creación de un perfil CalDAV

Antes de empezar:

- Compruebe que el dispositivo pueda acceder a un servidor CalDAV activo.

1. En la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Correo, Calendario y contactos > CalDAV**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil.
5. Escriba la dirección del servidor para el perfil. Es el FQDN del equipo que aloja la aplicación Calendario.
6. En el campo **Nombre de usuario**, realice una de las siguientes acciones:
   - Si el perfil es para un usuario, escriba el nombre de usuario.
   - Si el perfil es para varios usuarios, escriba `%UserName%`.
7. Si es necesario, introduzca el puerto para el servidor CalDAV.
8. Si es necesario, seleccione la casilla de verificación **Utilizar SSL** e introduzca la URL para el servidor SSL.
9. Haga clic en **Agregar**.

Después de terminar: Asigne el perfil a los usuarios, a los grupos de usuarios o a los grupos de dispositivos.

Tareas relacionadas

Asignación de un perfil o una política de TI a un grupo de usuarios
Asignar un perfil o una política de TI a una cuenta de usuario

Certificados

Un certificado es un documento digital emitido por una CA que verifica la identidad del sujeto del certificado y vincula la identidad a una clave pública. Cada certificado tiene una clave privada correspondiente que se almacena por separado. La clave pública y la privada forman un par de claves asimétricas que se pueden utilizar para el cifrado de datos y la autenticación de identidad. Una autoridad de certificación (CA) firma el certificado para verificar que las entidades que confían en la autoridad de certificación también puedan confiar en el certificado.

En función de la capacidad del dispositivo y del tipo de activación, los dispositivos pueden utilizar los certificados para:

- Autenticar mediante SSL/TLS al conectarse a páginas web que utilizan HTTPS
- Autenticar con un servidor de correo del trabajo
- Autenticar con una red Wi-Fi de trabajo o de VPN
- Cifrar y firmar mensajes de correo mediante protección S/MIME

Varios de los certificados utilizados con distintos fines se pueden guardar en un dispositivo. Puede utilizar perfiles de certificados para enviar certificados de CA y de cliente a los dispositivos.

Pasos para utilizar certificados con dispositivos

Al utilizar certificados con dispositivos, realice las siguientes acciones:

Paso	Acción
1	Si es necesario, conecte BlackBerry UEM al software de PKI de su empresa.
2	Cree uno o más perfiles de certificados de CA para enviarlos a los dispositivos.
3	Cree SCEP, credenciales de usuario o perfiles de certificado compartido o cargue certificados para un usuario específico para enviar certificados de cliente a los dispositivos.
4	Si es necesario, asocie perfiles de certificado con perfiles de Wi-Fi , VPN o de correo.
5	Si es necesario, asigne los perfiles de certificado a las cuentas de usuario, a los grupos de usuarios o a los grupos de dispositivos.

Integración de BlackBerry UEM con el software PKI de la empresa

Si su empresa utiliza una solución de PKI, como el software Entrust o OpenTrust para proporcionar certificados, puede extender la autenticación basada en certificados proporcionada por los servicios de PKI a los dispositivos que gestiona con BlackBerry UEM.

Los productos de Entrust (por ejemplo, Entrust IdentityGuard y Entrust Authority Administration Services) y productos de OpenTrust (por ejemplo, OpenTrust PKI y OpenTrust CMS) proporcionan las CA que emiten

certificados de cliente. Puede configurar una conexión con el software PKI de la empresa y utilizar los perfiles para enviar el certificado de CA y los certificados de cliente a los dispositivos.

Para los dispositivos con BlackBerry Dynamics, también puede configurar un conector de PKI que crea una conexión entre BlackBerry UEM y un servidor CA para inscribir certificados para las aplicaciones de BlackBerry Dynamics o utilizar una aplicación compatible con inscripción de certificados basada en aplicación como Purebred.

Conectar BlackBerry UEM al software de Entrust de la empresa

Para ampliar la autenticación basada en certificados de Entrust a los dispositivos, debe agregar una conexión al software de Entrust de la empresa (por ejemplo, Entrust IdentityGuard o Entrust Authority Administration Services).

Antes de empezar: Póngase en contacto con el administrador de Entrust de la empresa para obtener:

- la URL del servicio web MDM de Entrust
- la información de inicio de sesión de una cuenta de administrador de Entrust que pueda usar para conectar BlackBerry UEM al software de Entrust
- el certificado de CA de Entrust que contiene la clave pública (.der, .pem, o .cert); BlackBerry UEM utiliza este certificado para establecer conexiones SSL con el servidor de Entrust

1. En la barra de menús, haga clic en **Configuración**.
2. Haga clic en **Integración externa > Autoridad de certificación**.
3. Haga clic en **Agregar una conexión Entrust**.
4. En el campo **Nombre de la conexión**, escriba un nombre para la conexión.
5. En el campo **URL**, escriba la URL del servicio web MDM de Entrust.
6. En el campo **Nombre de usuario**, escriba el nombre de usuario de la cuenta del administrador de Entrust.
7. En el campo **Contraseña**, escriba la contraseña de la cuenta del administrador de Entrust.
8. Para cargar un certificado de CA con el fin de permitir que BlackBerry UEM establezca conexiones SSL con el servidor de Entrust, haga clic en **Examinar**. Navegue y seleccione el certificado de CA.
9. Para probar la conexión, haga clic en **Probar conexión**.
10. Haga clic en **Guardar**.

Después de terminar:

- Cree un perfil de credenciales de usuario para enviar certificados de su software de PKI a los dispositivos.

Conectar BlackBerry UEM al servidor de Entrust IdentityGuard de su empresa para utilizar credenciales inteligentes

Si su empresa utiliza credenciales inteligentes derivadas gestionadas por Entrust IdentityGuard, puede utilizar credenciales inteligentes derivadas con dispositivos gestionados por BlackBerry UEM.

Antes de empezar:

- Compruebe que BlackBerry UEM se puede conectar al servidor de Entrust IdentityGuard. Si está utilizando la versión en la nube de Entrust IdentityGuard, puede que necesite abrir un puerto en el firewall.
- Póngase en contacto con el administrador de Entrust de la empresa para obtener la información siguiente:
  - URL del servidor de Entrust IdentityGuard
  - Nombre de la credencial inteligente que se va a activar en los dispositivos como se especifica en Entrust IdentityGuard
  - Certificado de CA de Entrust para enviar el certificado a los dispositivos

1. En la barra de menú, haga clic en **Configuración**.

2. Haga clic en **Integración externa > Autoridad de certificación**.
3. Haga clic en **Añadir una conexión para credenciales inteligentes de Entrust**.
4. En el campo **Nombre de la credencial inteligente**, escriba el nombre de la credencial inteligente que se especifica en Entrust IdentityGuard.
5. En el campo **URL de Entrust**, escriba la URL del servidor de Entrust IdentityGuard.
6. Haga clic en **Agregar**.

Después de terminar:

- Creación de un perfil de certificado de CA para enviar el certificado de CA de Entrust a los dispositivos y asignar el perfil a los mismos usuarios o grupos a los que está asignado el perfil de credenciales del usuario.
- Crear un perfil de credenciales de usuario para utilizar credenciales inteligentes de Entrust en los dispositivos.

Conectar BlackBerry UEM al software de OpenTrust de la empresa

Para ampliar la autenticación basada en certificados de OpenTrust a los dispositivos, debe agregar una conexión al software de OpenTrust de la empresa. BlackBerry UEM admite la integración con OpenTrust PKI 4.8.0 y posteriores y OpenTrust CMS 2.0.4 y posteriores.

Antes de empezar: Póngase en contacto con el administrador de OpenTrust de la empresa para obtener la URL del servidor de OpenTrust, el certificado por parte del cliente que contiene la clave privada (formato .pfx o .p12) y la contraseña del certificado.

1. En la barra de menú, haga clic en **Settings (Configuración)**.
2. Haga clic en **Integración externa > Autoridad de certificación**.
3. Haga clic en **Agregar una conexión OpenTrust**.
4. En el campo **Nombre de la conexión**, escriba un nombre para la conexión.
5. En el campo **URL**, escriba la URL del software de OpenTrust.
6. Haga clic en **Examinar**. Desplácese y seleccione el certificado por parte del cliente que puede utilizar BlackBerry UEM para autenticar la conexión al servidor de OpenTrust.
7. En el campo **Contraseña del certificado**, escriba la contraseña del certificado del servidor de OpenTrust.
8. Para probar la conexión, haga clic en **Probar conexión**.
9. Haga clic en **Save (Guardar)**.

Después de terminar:

- Cree un perfil de credenciales de usuario para enviar certificados de su software de PKI a los dispositivos.
- Cuando se utiliza la conexión de BlackBerry UEM con el software de OpenTrust para distribuir certificados a los dispositivos, puede haber un breve retraso en la validez de los certificados. Este retraso podría causar problemas con la autenticación de correo durante el proceso de activación del dispositivo. Para resolver este problema, en el software de OpenTrust, configure la CA de OpenTrust y establezca "Retrasar fecha de certificados (segundos)" en 180.

Conexión de BlackBerry UEM al conector de PKI de BlackBerry Dynamics de la empresa

Para utilizar el software de PKI de la empresa para inscribir certificados para las aplicaciones de BlackBerry Dynamics, puede configurar un conector de PKI de BlackBerry Dynamics para comunicarse con la CA y vincular BlackBerry UEM con el conector de PKI.

Antes de empezar: Configure un conector de PKI de BlackBerry Dynamics. Para obtener más información, consulte Configuración de conexiones de PKI para aplicaciones de BlackBerry Dynamics en el contenido de Configuración.

1. En la barra de menú, haga clic en **Configuración > Integración externa > Autoridad de certificación**.
2. Haga clic en **Agregar una conexión de PKI de BlackBerry Dynamics**.

3. En el campo **Nombre de la conexión**, escriba un nombre para la conexión.
4. En el campo **URL**, escriba la URL del conector de PKI.
5. Seleccione una de las siguientes opciones:
   - **Autenticar con nombre de usuario y contraseña**: elija esta opción si BlackBerry UEM se autentica con el conector de PKI de BlackBerry Dynamics mediante la autenticación basada en contraseña.
   - **Autenticar con certificado de cliente**: elija esta opción si BlackBerry UEM se autentica con el conector de PKI de BlackBerry Dynamics mediante la autenticación basada en certificado.
6. Si ha seleccionado **Autenticar con nombre de usuario y contraseña**, en los campos **Nombre de usuario** y **Contraseña**, escriba el nombre de usuario y la contraseña del conector de PKI de BlackBerry Dynamics.
7. Si ha seleccionado **Autenticar con certificado de cliente**, haga clic en **Examinar** para seleccionar y cargar un certificado que sea de confianza para el conector de PKI de BlackBerry Dynamics. En el campo **Contraseña del certificado de cliente**, escriba la contraseña del certificado.
8. Para probar la conexión, haga clic en **Probar conexión**.
9. Haga clic en **Save**.

Después de terminar:

- Cree un perfil de credenciales de usuario para enviar certificados de su software de PKI a los dispositivos.

Conexión de BlackBerry UEM a la solución PKI basada en aplicación de su empresa

Para utilizar la solución PKI basada en aplicación de su empresa, como Purebred, para inscribir certificados para aplicaciones de BlackBerry Dynamics, puede instalar la aplicación en dispositivos y permitir que las aplicaciones de BlackBerry Dynamics utilicen los certificados inscritos a través de la aplicación PKI. Esta opción solo es compatible con dispositivos iOS.

Antes de empezar: Verifique que la aplicación que recupera los certificados para su uso en las aplicaciones de BlackBerry Dynamics se encuentra en la lista de aplicaciones en BlackBerry UEM.

1. En la barra de menú, haga clic en **Configuración > Integración externa > Autoridad de certificación**.
2. Haga clic en **Añadir una conexión para los certificados basados en dispositivo**.
3. Seleccione la aplicación que recupera los certificados de la aplicación PKI para su uso en las aplicaciones de BlackBerry Dynamics. Para utilizar Purebred, seleccione BlackBerry UEM Client.
4. Haga clic en **Agregar**.

Después de terminar:

- Creación de perfiles de credenciales de usuario para certificados basados en aplicaciones.

Integración de certificados de cliente en los dispositivos

Muchos de los certificados utilizados con distintos fines se pueden guardar en un dispositivo. Puede proporcionar certificados de cliente a los dispositivos de varias maneras.

Cómo se agrega el certificado	Descripción	Dispositivos compatibles
Durante la activación del dispositivo	BlackBerry UEM envía los certificados a los dispositivos durante el proceso de activación. Los dispositivos utilizan estos certificados para establecer conexiones seguras entre el dispositivo y BlackBerry UEM.	Todos
Perfiles SCEP	Puede crear perfiles SCEP que los dispositivos pueden utilizar para conectarse y obtener certificados de cliente de la CA de su empresa mediante un servicio SCEP. Los dispositivos pueden utilizar estos certificados para realizar la autenticación basada en certificados desde el navegador y para conectarse a la red Wi-Fi, la VPN y el servidor de correo del trabajo.	• BlackBerry 10 • iOS • macOS • Android • Windows 10
Conexión a la solución de PKI de la empresa	Si su empresa utiliza una solución de PKI, como los productos de software de Entrust o OpenTrust para emitir y gestionar certificados, puede crear perfiles de credenciales de usuario que los dispositivos pueden utilizar para obtener certificados de cliente de la CA de su empresa. Los dispositivos con BlackBerry Dynamics utilizan estos certificados para la autenticación basada en certificados de las aplicaciones de BlackBerry Dynamics. Otros dispositivos utilizan estos certificados para realizar la autenticación basada en certificados desde el navegador y para conectarse a la red Wi-Fi de trabajo, la VPN del trabajo y el servidor de correo del trabajo.	• BlackBerry 10 • iOS • Android
Perfiles de certificado compartido	Los perfiles de certificado compartido especifican el certificado de cliente que BlackBerry UEM envía a los dispositivos iOS, macOS y Android. BlackBerry UEM envía el mismo certificado de cliente a todos los usuarios a los que se ha asignado el perfil. El administrador debe tener acceso al certificado y la clave privada para crear un perfil de certificado compartido.	• iOS • macOS • Android

Cómo se agrega el certificado	Descripción	Dispositivos compatibles
Envío de certificados de cliente a cuentas de usuario individuales	Puede agregar un certificado de cliente a una cuenta de usuario. BlackBerry UEM puede enviar el certificado a los dispositivos iOS y Android del usuario. Si el certificado se asocia con un perfil de credenciales de usuario, los dispositivos pueden utilizar estos certificados para conectarse a su red Wi-Fi de trabajo, VPN de trabajo y servidor de correo de trabajo. El administrador debe tener acceso al certificado y la clave privada para enviar el certificado del cliente al usuario.	• BlackBerry 10 • iOS • Android
Carga de usuarios en UEM Self-Service	Los usuarios pueden cargar certificados en BlackBerry UEM Self-Service. A continuación, BlackBerry UEM inserta el certificado en los dispositivos de los usuarios. Si el certificado se asocia con un perfil de credenciales de usuario, los dispositivos pueden utilizar estos certificados para conectarse a su red Wi-Fi de trabajo, VPN de trabajo y servidor de correo de trabajo.	• BlackBerry 10 • iOS • Android
Importación por parte de los usuarios	Los usuarios pueden importar los certificados de cliente al almacén de certificados del dispositivo en la sección "Seguridad y privacidad" de "Configuración del sistema". Los certificados que se van a utilizar en el navegador de trabajo o bien para enviar mensajes protegidos con S/MIME desde la cuenta de correo de trabajo pueden importarse desde el sistema de archivos en el dispositivo o desde una ubicación de red a la que se puede acceder desde el espacio de trabajo.	BlackBerry 10
Tarjetas inteligentes	Los usuarios pueden importar certificados S/MIME y SSL a sus dispositivos desde una tarjeta inteligente.	BlackBerry 10

Envío de certificados a dispositivos mediante perfiles

Puede enviar certificados a los dispositivos utilizando los siguientes perfiles disponibles en la biblioteca Políticas y perfiles:

Perfil	Descripción
Certificado de CA	Los perfiles de certificado de CA especifican un certificado de CA que los dispositivos pueden utilizar para confiar en la identidad asociada con cualquier certificado de cliente o servidor que la CA haya firmado.
Credenciales de usuario	Los perfiles de credenciales de usuario envían certificados a los dispositivos de las siguientes formas: • Pueden especificar una conexión al software de PKI de su empresa para enviar certificados de cliente a los dispositivos. • Pueden permitirle cargar manualmente certificados en BlackBerry UEM y permitir que los usuarios carguen certificados utilizando BlackBerry UEM Self-Service.
SCEP	Los perfiles SCEP especifican cómo los dispositivos se conectan y obtienen certificados de clientes de la CA de la empresa mediante un servicio SCEP.
Certificado compartido	Los perfiles de certificado compartido especifican un certificado de cliente que BlackBerry UEM envía a los dispositivos iOS y Android. BlackBerry UEM envía el mismo certificado de cliente a todos los usuarios a los que se ha asignado el perfil.

Para los dispositivos iOS y Android, también puede enviar un certificado de cliente a un dispositivo agregándolo directamente a una cuenta de usuario. Para obtener más información, consulte Adición de un certificado de cliente a una cuenta de usuario.

Para los dispositivos con BlackBerry 10, iOS y Android, si la empresa utiliza certificados de S/MIME, también puede usar perfiles para permitir que los dispositivos puedan obtener claves públicas del destinatario y comprobar el estado del certificado. Para obtener más información, consulte Ampliación de la seguridad del correo mediante S/MIME.

En BlackBerry Dynamics, para utilizar certificados enviados por perfiles, debe seleccionar "Permitir que las aplicaciones de BlackBerry Dynamics utilicen certificados de usuario, perfiles SCEP y perfiles de credenciales de usuario" en la configuración de la aplicación.

Conceptos relacionados

Ampliación de la seguridad del correo mediante S/MIME

Tareas relacionadas

Adición de un certificado de cliente a una cuenta de usuario

Elección de perfiles para enviar certificados de cliente a los dispositivos

Puede utilizar diferentes tipos de perfiles para enviar certificados de cliente a los dispositivos. El tipo de perfil que seleccione dependerá de cómo su empresa utilice los certificados y los tipos de dispositivos que admita la empresa. Considere las siguientes directrices:

- Para utilizar perfiles SCEP, debe tener una CA que admita SCEP.
- Si ha configurado una conexión entre BlackBerry UEM y la solución PKI de la empresa, utilice los perfiles de credenciales de usuario para enviar certificados a los dispositivos. Puede conectarse directamente a una

CA de Entrust o CA de OpenTrust. También puede utilizar un conector de PKI de BlackBerry Dynamics para conectarse a un servidor CA a fin de inscribir certificados para dispositivos con BlackBerry Dynamics.

- Para permitir que los usuarios carguen certificados que puedan utilizar para conectarse a su red Wi-Fi de trabajo, red VPN de trabajo y servidor de correo del trabajo, utilice un perfil de credenciales de usuario.
- Para utilizar certificados con aplicaciones de BlackBerry Dynamics, debe utilizar un perfil de credenciales de usuario o agregar certificados a cuentas de usuario individuales.
- Para utilizar certificados de cliente para Wi-Fi, VPN y autenticación del servidor de correo, debe asociar el perfil de certificado con un perfil Wi-Fi, VPN o de correo electrónico.

  Nota: Los dispositivos Android Enterprise no son compatibles con el uso de los certificados que BlackBerry UEM ha enviado a los dispositivos para la autenticación Wi-Fi.
- Los perfiles de certificado compartido y los perfiles que agrega a las cuentas de usuario no mantienen la clave privada en privado porque se debe tener acceso a ella. La conexión a un CA mediante perfiles de credenciales de usuario o SCEP es más segura porque la clave privada solo se envía al dispositivo para el que se emitió el certificado.

Envío de certificados de CA a los dispositivos

Es posible que necesite enviar certificados de CA en los dispositivos si la empresa utiliza S/MIME o si los dispositivos utilizan autenticación basada en certificados para conectarse a una red o un servidor en el entorno de la empresa.

Cuando envía un certificado de CA a un dispositivo, el dispositivo confía en la identidad asociada a cualquier cliente o servidor certificado firmado por la CA. Cuando el certificado de la CA que ha firmado los certificados de red y servidor de la empresa se guarda en los dispositivos, estos pueden confiar en sus redes y servidores al establecer conexiones seguras. Cuando el certificado de la CA que ha firmado los certificados S/MIME de la empresa se guarda en los dispositivos, los dispositivos pueden confiar en el certificado del remitente al recibir un mensaje de correo seguro.

Varios de los certificados de CA que se utilizan con distintos fines se pueden guardar en un dispositivo. Puede utilizar perfiles de certificados de CA para enviar certificados de CA a los dispositivos.

Creación de un perfil de certificado de CA

Antes de empezar: Debe obtener el archivo del certificado de CA que desea enviar a los dispositivos.

1. En la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Certificados > Certificado de CA**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil. Cada perfil de certificado de CA debe tener un nombre único. Algunos nombres (por ejemplo, ca_1) están reservados.
5. En el campo **Archivo de certificado**, haga clic en **Examinar** para ubicar el archivo de certificado.
6. Si el certificado de CA se envía a los dispositivos BlackBerry 10, en la pestaña BlackBerry, especifique uno o más de los siguientes almacenes de certificados para enviar el certificado al dispositivo:
   - Almacén de certificados del navegador
   - Almacén de certificados VPN
   - Almacén de certificados Wi-Fi
   - Almacén de certificados de empresa
7. Si el certificado CA se envía a los dispositivos macOS, en la pestaña macOS, en la lista desplegable **Aplicar perfil a**, seleccione **Usuario** o **Dispositivo**.
8. Haga clic en **Agregar**.

Tareas relacionadas

Asignar un perfil o una política de TI a una cuenta de usuario
Asignación de un perfil o una política de TI a un grupo de usuarios

Almacenes de certificados de CA en los dispositivos con BlackBerry 10

Los certificados de CA que se envían a los dispositivos con BlackBerry 10 se guardan en distintos almacenes de certificados, dependiendo del propósito del certificado.

Almacén	Descripción
Almacén de certificados del navegador	El navegador de trabajo en los dispositivos con BlackBerry 10 utiliza los certificados de este almacén para establecer conexiones SSL con los servidores del entorno de la empresa.
Almacén de certificados VPN	Los dispositivos con BlackBerry 10 utilizan los certificados de este almacén para las conexiones VPN. Debe establecer el ajuste "Origen del certificado de confianza" del perfil VPN en "Almacén de certificados de confianza" con el fin de utilizar los certificados de este almacén en las conexiones VPN de la empresa.
Almacén de certificados Wi-Fi	Los dispositivos con BlackBerry 10 utilizan los certificados de este almacén para las conexiones Wi-Fi. Debe establecer el ajuste "Origen del certificado de confianza" del perfil de Wi-Fi en "Almacén de certificados de confianza" con el fin de utilizar los certificados de este almacén en las conexiones Wi-Fi de trabajo de la empresa.
Almacén de certificados de empresa	Los dispositivos con BlackBerry 10 emplean los certificados de este almacén para autenticar los mensajes de correo protegidos por S/MIME que se reciban.

Uso de perfiles de credenciales de usuario para enviar certificados a los dispositivos

Los perfiles de credenciales de usuario permiten a los dispositivos obtener certificados de cliente de la CA de su empresa. También pueden permitirle cargar manualmente certificados en BlackBerry UEM y permitir que los usuarios carguen certificados utilizando BlackBerry UEM Self-Service.

BlackBerry UEM se puede conectar directamente a la CA de Entrust o CA de OpenTrust de su empresa. Para los dispositivos con BlackBerry Dynamics, también puede configurar un conector de PKI para que se conecte a un servidor CA a fin de inscribir certificados para aplicaciones de BlackBerry Dynamics o utilizar una solución PKI basada en aplicación como Purebred.

Si los usuarios cargan los certificados manualmente en UEM Self-Service, puede ver el certificado en la página de usuario de la consola de gestión. También puede eliminar o sustituir el certificado.

Los perfiles de credenciales de usuario son compatibles con dispositivos iOS y Android, y con dispositivos con BlackBerry 10 OS versión 10.3.1 y posterior. Las soluciones PKI basadas en aplicación son compatibles con dispositivos iOS. La carga manual de certificados es compatible con dispositivos BlackBerry 10 y iOS, y con dispositivos Android con un perfil de trabajo y dispositivos Samsung KNOX Workspace.

Para obtener más información sobre la conexión de BlackBerry UEM al software de PKI de su empresa, consulte Integración de BlackBerry UEM con el software PKI de la empresa.

De manera alternativa, puede utilizar perfiles SCEP para inscribir los certificados de cliente en los dispositivos. También puede cargar certificados directamente en una cuenta de usuario. El tipo de perfil que seleccione

dependerá de cómo su empresa utilice el software PKI, los tipos de dispositivos que admita la empresa y cómo desee administrar certificados.

Cree un perfil de credenciales de usuario para cargar manualmente los certificados

Los perfiles de credenciales de usuario permiten cargar manualmente un certificado que se enviará a los dispositivos del usuario.

1. En la barra de menú, haga clic en **Policies and Profiles (Políticas y perfiles)**.
2. Haga clic en **Certificados > Credenciales de usuario**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil. Cada perfil de certificado debe tener un nombre único.
5. En la lista desplegable **Conexión con la autoridad de certificación**, seleccione **Certificado cargado manualmente**.
6. Haga clic en **Agregar**.

Después de terminar:

- Si los dispositivos utilizan los certificados de cliente para autenticarse con una red Wi-Fi, una VPN o un servidor de correo, asocie el perfil de credenciales de usuario a un perfil Wi-Fi, de VPN o de correo.
- Asigne el perfil a las cuentas de usuario y los grupos de usuarios.
- Adición de un certificado de cliente a un perfil de credenciales de usuario o indique a los usuarios que utilicen BlackBerry UEM Self-Service para cargar su propio certificado.

Tareas relacionadas

Adición de un certificado de cliente a un perfil de credenciales de usuario
Cambie un certificado de cliente por un perfil de credenciales de usuario

Creación de un perfil de credenciales de usuario para conectarse al software de PKI de su empresa

Antes de empezar:

- Contacte con el administrador de Entrust o de OpenTrust de la empresa para confirmar qué perfil de PKI debe seleccionar. BlackBerry UEM obtiene una lista de perfiles del software PKI.
- Solicite al administrador de Entrust o OpenTrust los valores para el perfil que debe proporcionar. Por ejemplo, los valores del tipo de dispositivo (devicetype), grupo de Entrust IdentityGuard (iggroup) y nombre de usuario de Entrust IdentityGuard (igusername).
- Si el sistema OpenTrust de su empresa está configurado para devolver solo claves bajo custodia, el administrador de OpenTrust debe verificar que haya certificados para cada usuario en el sistema OpenTrust. Al asignar un perfil de credenciales de usuario a los usuarios en BlackBerry UEM no se crean automáticamente certificados para usuarios en OpenTrust. En este caso, un perfil de credenciales de usuario solo puede distribuir certificados a los usuarios que tienen un certificado existente en el sistema OpenTrust.

1. En la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Certificados > Credenciales de usuario**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil. Cada perfil de certificado debe tener un nombre único.
5. En la lista desplegable **Conexión con la autoridad de certificación**, haga clic en la conexión de Entrust o OpenTrust que configuró.
6. En la lista desplegable **Perfil**, haga clic en el perfil adecuado.

7. Especifique los valores para el perfil.
8. Si es necesario, puede especificar un tipo de SAN y un valor para un certificado de cliente de Entrust.
   a) En la tabla de SAN, haga clic en +.
   b) En la lista desplegable **Tipo de SAN**, haga clic en el tipo adecuado.
   c) En el campo **Valor de SAN**, escriba el valor de SAN.

      Si se establece el tipo de SAN en "Nombre de RFC822", el valor debe ser una dirección de correo válida. Si se establece en "URI", el valor debe ser una URL válida que incluya el protocolo y la dirección IP o FQDN. Si se establece en "Nombre principal de NT", el valor debe ser un nombre principal válido. Si se establece en "Nombre de DNS", el valor debe ser un FQDN válido.
9. Especifique el **Período de renovación** del certificado. El período puede ser entre 1 y 120 días.
10. Si los dispositivos con BlackBerry 10 utilizan el certificado de cliente para cifrar mensajes de correo mediante S/MIME y desea que conserven el acceso a los certificados caducados para que los usuarios puedan abrir los mensajes de correo antiguos, seleccione la casilla de verificación **Incluir historial del certificado**.
11. Haga clic en **Agregar**.

Después de terminar:

- Si los dispositivos utilizan los certificados de cliente para autenticarse con una red Wi-Fi, una VPN o un servidor de correo, asocie el perfil de credenciales de usuario a un perfil Wi-Fi, de VPN o de correo.
- Asigne el perfil a las cuentas de usuario y los grupos de usuarios. Se les solicita a los usuarios de Android que introduzcan una contraseña cuando reciben el perfil (la contraseña se muestra en pantalla).

Tareas relacionadas

Asignación de un perfil o una política de TI a un grupo de usuarios
Asignar un perfil o una política de TI a una cuenta de usuario

Crear un perfil de credenciales de usuario para utilizar credenciales inteligentes de Entrust en los dispositivos

Las credenciales inteligentes derivadas de Entrust son compatibles con las siguientes aplicaciones:

- Aplicaciones de BlackBerry Dynamics en dispositivos iOS
- Aplicaciones de BlackBerry Dynamics en dispositivos Android que no sean dispositivos Samsung KNOX Workspace
- Aplicaciones en dispositivos Android con un perfil de trabajo que utilice certificados para firma, cifrado y autenticación de identidad, como BlackBerry Hub y los navegadores web compatibles
- Aplicaciones en dispositivos Samsung KNOX Workspace que utilizan certificados para firma, cifrado y autenticación de identidad, como el cliente de correo nativo de Samsung y los navegadores web compatibles

Nota: BlackBerry UEM no es compatible con el historial de claves para credenciales inteligentes derivadas.

Antes de empezar:

- Conectar BlackBerry UEM al servidor de Entrust IdentityGuard de su empresa para utilizar credenciales inteligentes.
- Creación de un perfil de certificado de CA para enviar el certificado de CA de Entrust a los dispositivos y asignar el perfil a los mismos usuarios o grupos a los que está asignado este perfil de credenciales del usuario.

1. En la barra de menú, haga clic en **Políticas y perfiles**.
2. Haga clic en **Certificados > Credenciales de usuario**.
3. Haga clic en +.

4. Escriba un nombre y una descripción para el perfil. Cada perfil de certificado debe tener un nombre único.
5. En la lista desplegable **Conexión con la autoridad de certificación**, seleccione la conexión de credenciales inteligentes de Entrust que ha configurado.
6. En la lista desplegable **Tipo de certificado**, especifique si la credencial inteligente se utilizará para autenticación de identidad, firma o cifrado.

   Si desea enviar credenciales inteligentes a aplicaciones para más de un fin, cree perfiles de credenciales de usuario adicionales.
7. Si la credencial inteligente se enviará a dispositivos Samsung KNOX Workspace o a aplicaciones que no sean las aplicaciones de BlackBerry Dynamics en dispositivos Android con un perfil de trabajo, haga clic en la pestaña **Android** y seleccione **Entregar a llavero nativo**.

   Si no se selecciona esta opción, solo las aplicaciones de BlackBerry Dynamics pueden utilizar la credencial inteligente.
8. Si la credencial inteligente se enviará a aplicaciones de BlackBerry Dynamics, haga clic en la pestaña **BlackBerry Dynamics** y lleve a cabo las acciones siguientes:
   a) Si desea que el dispositivo elimine credenciales duplicadas, seleccione **Eliminar certificados duplicados**. El dispositivo elimina la credencial que tiene la fecha de inicio más inmediata.
   b) Si desea que el dispositivo elimine credenciales caducadas, seleccione **Eliminar certificados caducados**.
   c) Para permitir que todas las aplicaciones de BlackBerry Dynamics utilicen las credenciales inteligentes, seleccione **Permitir que todas las aplicaciones utilicen certificados**.
   d) Para especificar las aplicaciones de BlackBerry Dynamics que utilizan las credenciales inteligentes, seleccione **Permitir que aplicaciones específicas utilicen certificados** ya haga clic en + para especificar las aplicaciones. Debe incluir BlackBerry UEM Client en la lista de aplicaciones.
9. Haga clic en **Agregar**.

Después de terminar:

- Asigne el perfil a las cuentas de usuario y los grupos de usuarios.
- Después de que un dispositivo reciba el perfil, los usuarios deben iniciar sesión en el módulo de autoservicio de Entrust IdentityGuard para activar su credencial inteligente y utilizar BlackBerry UEM Client para escanear el código QR presentado por el módulo de autoservicio de Entrust IdentityGuard y agregar la credencial inteligente al dispositivo.
- Para eliminar una credencial inteligente de Entrust de un dispositivo, el usuario debe desactivar la credencial inteligente en BlackBerry UEM Client antes de anular la asignación del perfil o eliminar el certificado.

Creación de un perfil de credenciales de usuario para conectarse al conector de PKI de BlackBerry Dynamics

1. En la barra de menú, haga clic en **Policies and Profiles (Políticas y perfiles)**.
2. Haga clic en **Certificados > Credenciales de usuario**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil. Cada perfil de certificado debe tener un nombre único.
5. En la lista desplegable **Conexión con la autoridad de certificación**, seleccione la conexión de PKI de BlackBerry Dynamics que ha configurado.
6. Si el usuario debe proporcionar una contraseña para solicitar un certificado, seleccione **Requerir contraseña introducida por el usuario u OTP**.
7. Si desea permitir que el dispositivo solicite automáticamente un nuevo certificado antes de que el certificado actual caduque, seleccione **Activar la renovación de certificados** y especifique el número de días previos a la caducidad en que los dispositivos deben solicitar un nuevo certificado.
8. Si desea que el dispositivo elimine certificados caducados, seleccione **Eliminar certificados caducados**.

9. Si desea que el dispositivo elimine certificados duplicados, seleccione **Eliminar certificado duplicado**. El dispositivo elimina el certificado que tiene la fecha de inicio más inmediata.
10. Haga clic en **Agregar**.

Después de terminar:

- Permita que las aplicaciones de BlackBerry Dynamics usen certificados.
- Asigne el perfil a las cuentas de usuario y los grupos de usuarios.
- Si actualiza el conector PKI, haga clic en **Actualizar capacidades de PKI** para actualizar las funciones PKI admitidas para el perfil.

Renovación de certificados que están escritos mediante el conector de PKI de BlackBerry Dynamics

Si necesita actualizar los certificados de usuario de todos los usuarios de BlackBerry Dynamics, puede enviar un comando para solicitar la renovación de los certificados a todos los dispositivos que tengan asignado el perfil de credenciales de usuario.

1. En la barra de menú, haga clic en **Policies and Profiles (Políticas y perfiles)**.
2. Haga clic en **Certificados > Credenciales de usuario**.
3. Haga clic en el nombre del perfil que desea cambiar.
4. Haga clic en **Actualizar capacidades de PKI** para asegurarse de que BlackBerry UEM tiene los detalles más recientes del conector de PKI.
5. Haga clic en **Renovar** para ordenar a todos los dispositivos con BlackBerry Dynamics que tengan asignado el perfil que soliciten la renovación de certificados.

Tareas relacionadas

Renovación o eliminación de un certificado de BlackBerry Dynamics para una cuenta de usuario

Creación de perfiles de credenciales de usuario para certificados basados en aplicaciones

Para utilizar la solución PKI basada en aplicación de su empresa, como Purebred, para inscribir certificados para aplicaciones de BlackBerry Dynamics, puede instalar la aplicación en dispositivos y permitir que las aplicaciones de BlackBerry Dynamics utilicen los certificados inscritos a través de la aplicación PKI. Esta opción solo es compatible con dispositivos iOS.

Si envía más de un certificado a los dispositivos, considere la configuración de varios perfiles de credenciales de usuario e incluya un tipo diferente de certificado en cada perfil. La configuración de varios perfiles ofrece las siguientes ventajas:

- Cuando Microsoft Exchange se configura para autenticación basada en certificados cliente, BlackBerry Work utiliza un nombre de perfil de credenciales de usuario configurado para identificar de forma inequívoca el certificado de autenticación. Esto no es posible si utiliza un solo perfil de credenciales de usuario.
- Con un solo perfil de credenciales de usuario para varios certificados, no hay indicación en caso de que falten certificados. Por ejemplo, si un usuario necesita un certificado de cifrado y solo se importan certificados de firma y autenticación, BlackBerry UEM Client indica que la importación se ha realizado correctamente. Sin embargo, si configura perfiles de credenciales de usuario independientes y falta el certificado de cifrado, BlackBerry UEM Client indica al usuario que falta el certificado.

Requisitos previos: creación de un perfil de credenciales de usuario para usar certificados basados en aplicaciones

Antes de crear un perfil de credenciales de usuario para usar la solución PKI basada en aplicación de su empresa, como Purebred, lleve a cabo las siguientes acciones:

- Creación de un perfil de BlackBerry Dynamics. En el perfil, seleccione **Activar UEM Client para que pueda inscribirse en BlackBerry Dynamics** y seleccione BlackBerry UEM Client para **Delegación de autenticación de aplicaciones**.
- Conexión de BlackBerry UEM a la solución PKI basada en aplicación de su empresa
- Configuración de BlackBerry UEM Client para que sea compatible con certificados basados en aplicación
- Configuración de las aplicaciones de BlackBerry Dynamics para utilizar certificados basados en aplicación
- Asegúrese de que la aplicación PKI (por ejemplo, Purebred) está instalada en los dispositivos de los usuarios.

Configuración de BlackBerry UEM Client para que sea compatible con certificados basados en aplicación

1. En la consola de administración de BlackBerry UEM, haga clic en la opción **Aplicaciones** de la barra de menú.
2. En la lista de aplicaciones, seleccione BlackBerry UEM Client.
3. En la sección Configuración de aplicación, haga clic en +.
4. En el campo **Nombre de aplicación**, escriba un nombre para la aplicación.
5. En el campo **UTI schemes**, especifique los esquemas de UTI de la solución PKI basada en aplicación de su empresa. Por ejemplo, si utiliza la aplicación Purebred, use los esquemas siguientes: purebred.zip.all, purebred.zip.no_filter.
6. Haga clic en **Guardar**.
7. Seleccione **Permitir que las aplicaciones de BlackBerry Dynamics utilicen certificados de usuario y perfiles de credenciales de usuario**.
8. Asigne BlackBerry UEM Client con la configuración de aplicación que ha creado a los usuarios y dispositivos que desea que utilicen la solución PKI basada en aplicación.

Configuración de las aplicaciones de BlackBerry Dynamics para utilizar certificados basados en aplicación

1. En la consola de administración de BlackBerry UEM, haga clic en la opción **Aplicaciones** de la barra de menú.
2. En la lista de aplicaciones, seleccione la aplicación (por ejemplo, BlackBerry Work o BlackBerry Access).
3. Seleccione la opción **Permitir que las aplicaciones de BlackBerry Dynamics utilicen certificados de usuario y perfiles de credenciales de usuario**.
4. Si va a configurar BlackBerry Work, en la sección Configuración de aplicación, haga clic en + y lleve a cabo una de las tareas siguientes:

Tarea	Pasos
Configurar BlackBerry Work cuando su empresa utiliza BEMS	a. En la pestaña Configuration Settings, seleccione **Clients must have individual login certificates (SSL) uploaded in the GC**. b. Para activar la autodetección del servidor de Microsoft Exchange en el que se encuentran los usuarios, seleccione **Use BEMS to perform Autodiscover of the EAS/EWS endpoint for the user**. c. En la pestaña **Exchange Settings**, en el campo **User Credential Profile Name**, escriba del nombre del perfil de credenciales de usuario.

Tarea	Pasos
Configurar BlackBerry Work cuando su empresa no utiliza BEMS	**a.** Seleccione la pestaña **Exchange Settings**. **b.** Si el servidor utiliza el formato de inicio de sesión *nombre de dominio\usuario*, en el campo **Dominio predeterminado**, especifique el dominio de Windows NT predeterminado al que se conecta BlackBerry Work cuando los usuarios inician sesión. **c.** En el campo **Active Sync Server**, especifique el servidor de Exchange ActiveSync predeterminado al que BlackBerry Work se conecta cuando los usuarios inician sesión en BlackBerry Work (por ejemplo, cas.mydomain.com). **d.** En el campo **Auto Discover URL**, especifique la URL de autodetección si la sabe. Esto acelera el proceso de configuración de autodetección (por ejemplo, https://autodiscover.mydomain.com). **e.** En el campo **Auto Discover Connection Timeout in Seconds (iOS only)**, especifique el tiempo de espera de conexión de autodetección en segundos. **f.** En el campo **User Credential Profile Name**, escriba del nombre del perfil de credenciales de usuario.

5. Haga clic en **Guardar**.

Creación de un perfil de credenciales de usuario para usar certificados basados en aplicaciones

1. En la barra de menú, haga clic en **Policies and Profiles (Políticas y perfiles)**.
2. Haga clic en **Certificados > Credenciales de usuario**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil. Cada perfil de certificado debe tener un nombre único.
5. En la lista desplegable **Conexión con la autoridad de certificación**, seleccione el nombre de la aplicación que especificó al conectar BlackBerry UEM a su solución PKI. Si utiliza Purebred, seleccione BlackBerry UEM Client
6. En la sección **Uso de la clave**, seleccione las operaciones con las que es compatible el certificado.

   Por ejemplo, puede seleccionar **Cifrado de clave** para un certificado de cifrado, **Firma digital** para un certificado de autenticación y **Firma digital** y **No rechazo** para un certificado de firma.
7. En la sección **Uso extendido de la clave**, seleccione las funciones para las que los usuarios utilizarán el certificado.
8. Si el certificado se va a utilizar para fines distintos a correo electrónico, autenticación de cliente o inicio de sesión de tarjeta inteligente, seleccione **Uso de ID de objeto adicional**, haga clic en + y especifique el OID del uso de la clave. Por ejemplo, si el certificado se va a utilizar para autenticación de servidor, agregue el OID 1.3.6.1.5.5.7.3.1.
9. Si desea especificar el emisor del certificado, junto a **Emisores**, haga clic en + y escriba el nombre del emisor. El nombre del emisor debe coincidir con el nombre de OID corto de OpenSSL. Puede copiar este valor del certificado del emisor. No incluya espacios antes o después del signo "=". Por ejemplo:

   ```
   CN=Acme_cert SMIME,OU=Acme_Legal,O=Acme,C=Can
   CN=Acme_cert SMIME,OU=Acme_Legal,O=Acme
   CN=Acme_cert TLS
   ```
10. Si desea que el dispositivo elimine certificados caducados, seleccione **Eliminar certificados caducados**.

    Los certificados de cifrado caducados utilizados para S/MIME deben conservarse en el dispositivo para que los usuarios puedan leer los mensajes cifrados antes de la caducidad del certificado de cifrado.

11. Si desea que el dispositivo elimine certificados duplicados, seleccione **Eliminar certificado duplicado**. El dispositivo elimina el certificado que tiene la fecha de inicio más inmediata.
12. Haga clic en **Agregar**.

Después de terminar:

- Permita que las aplicaciones de BlackBerry Dynamics usen certificados.
- Asigne el perfil a las cuentas de usuario y los grupos de usuarios.

Crear un perfil de credenciales de usuario para utilizar certificados del almacén de claves nativo en dispositivos Android

Puede configurar el perfil de certificado de usuario para permitir que las aplicaciones de BlackBerry Dynamics puedan utilizar un certificado del almacén de claves nativo en dispositivos Android. Puede permitir que las aplicaciones de BlackBerry Dynamics utilicen cualquier certificado agregado al almacén de claves o definir restricciones de los certificados que puede escoger la aplicación. Por ejemplo, si está utilizando una solución PKI basada en aplicación como Purebred, que añade certificados al almacén de claves nativo, puede forzar la aplicación para que seleccione un certificado emitido por su solución PKI Purebred y obligar a que la aplicación utilice certificados con capacidades específicas.

1. En la barra de menú, haga clic en **Políticas y perfiles**.
2. Haga clic en **Certificados > Credenciales de usuario**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil. Cada perfil de certificado debe tener un nombre único.
5. En la lista desplegable **Conexión con la autoridad de certificación**, seleccione **Almacén de claves nativo**.
6. Para especificar qué certificado utilizará la aplicación de BlackBerry Dynamics, realice las acciones siguientes:
   a) Junto a **Emisores**, haga clic en + y escriba el nombre del emisor.

      Las aplicaciones de BlackBerry Dynamics solo utilizarán un certificado si el emisor especificado coincide con el OID abreviado de OpenSSL en el certificado. Puede copiar este valor del certificado del emisor. No incluya espacios antes o después del signo igual (=). Por ejemplo:

      ```
      CN=Acme_cert SMIME,OU=Acme_Legal,O=Acme,C=Can
                        CN=Acme_cert SMIME,OU=Acme_Legal,O=Acme
                        CN=Acme_cert TLS
      ```

   b) En la sección **Uso de la clave**, seleccione las operaciones con las que es compatible el certificado.

      Las aplicaciones de BlackBerry Dynamics solo utilizarán certificados en los que se haya especificado al menos el valor de uso de la clave. Por ejemplo, un certificado de cifrado puede tener un valor de uso de la clave de **Cifrado de clave**. Un certificado de autenticación puede tener un valor de uso de la clave de **Firma digital**. Un certificado de firma puede tener un valor de uso de la clave de **Firma digital** y **No rechazo**.
   c) En la sección **Uso extendido de la clave**, seleccione las funciones para las que se emitió el certificado.

      Las aplicaciones de BlackBerry Dynamics solo utilizarán certificados si todos los valores de uso de la clave ampliados seleccionados están presentes en el certificado. Los certificados pueden tener más valores de uso de la clave ampliados.
   d) Si el certificado se emitió para fines distintos al uso en correo electrónico, la autenticación de cliente y el inicio de sesión con tarjeta inteligente, seleccione **Uso de ID de objeto adicional**, haga clic en + y especifique el OID del uso de la clave. Por ejemplo, si el certificado se va a utilizar para autenticación de servidor, puede tener el OID 1.3.6.1.5.5.7.3.1
7. Si desea que el dispositivo elimine certificados caducados, seleccione **Eliminar certificados caducados**.

   Los certificados de cifrado caducados utilizados para S/MIME deben conservarse en el dispositivo para que los usuarios puedan leer los mensajes cifrados antes de la caducidad del certificado de cifrado.

8. Si desea que el dispositivo elimine certificados duplicados, seleccione **Eliminar certificado duplicado**. El dispositivo elimina el certificado que tiene la fecha de inicio más inmediata.
9. Haga clic en **Agregar**.

Después de terminar:

- Permita que las aplicaciones de BlackBerry Dynamics usen certificados.
- Asigne el perfil a las cuentas de usuario y los grupos de usuarios.

Uso de SCEP para enviar certificados de cliente a los dispositivos

Puede utilizar perfiles SCEP para especificar cómo los dispositivos con BlackBerry 10, los dispositivos iOS, los dispositivos Android y los dispositivos con Windows 10 obtienen certificados de cliente de la CA de la empresa a través de un servicio SCEP. SCEP es un protocolo IETF que simplifica el proceso de inscripción de certificados de cliente en un gran número de dispositivos sin necesidad de ninguna introducción de datos o aprobación por parte del administrador para emitir cada certificado. Los dispositivos pueden usar SCEP para solicitar y obtener certificados de cliente de una CA compatible con SCEP que utilice la empresa. La CA que utilice debe admitir contraseñas de comprobación. La CA utiliza contraseñas de comprobación para verificar que el dispositivo esté autorizado a enviar una solicitud de certificado.

Dependiendo de la capacidad del dispositivo y el tipo de activación, los dispositivos pueden usar los certificados de cliente obtenidos mediante SCEP para autenticación basada en certificados desde el navegador o para conectarse a una red Wi-Fi de trabajo, VPN de trabajo o servidor de correo.

Si su empresa utiliza una CA de Entrust o CA de OpenTrust, los perfiles de SCEP no son compatibles para los dispositivos con Windows 10.

Crear un perfil SCEP

La configuración del perfil requerida varía para cada tipo de dispositivo y depende de la configuración del servicio SCEP aplicada en el entorno de su empresa.

Nota: Si desea utilizar un perfil SCEP para distribuir certificados de cliente de OpenTrust a los dispositivos, debe realizar una revisión de su OpenTrust software. Para obtener más información, póngase en contacto con su representante de soporte de OpenTrust y consulte el caso de soporte SUPPORT-798.

1. En la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Certificados > SCEP**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil. Cada perfil de certificado debe tener un nombre único.
5. En el campo **URL**, escriba la URL para el servicio SCEP. La URL debe incluir el protocolo, FQDN, el número de puerto y la ruta SCEP.
6. En el campo **Nombre de la instancia**, escriba el nombre de la instancia para la CA.
7. En la lista desplegable **Conexión con la autoridad de certificación**, lleve a cabo una de las acciones siguientes:
   - Para utilizar una conexión Entrust que haya configurado, haga clic en la conexión correspondiente. En la lista desplegable **Perfil**, haga clic en un perfil. Especifique los valores para el perfil.
   - Para utilizar una conexión OpenTrust que haya configurado, haga clic en la conexión correspondiente. En la lista desplegable**Perfil**, haga clic en un perfil. Especifique los valores para el perfil.
     - Las siguientes opciones del perfil SCEP no se aplican a los certificados de cliente de OpenTrust: Uso de la clave, Uso extendido de la clave, Asunto y SAN.
   - Para utilizar otra CA, haga clic en **Genérico**. En la lista desplegable **Tipo de desafío SCEP**, seleccione **Estático** o **Dinámico** y especifique los ajustes necesarios para el tipo de desafío.

     Nota: Para los dispositivos Windows, únicamente se admiten contraseñas estáticas.

8. Opcionalmente, desactive la casilla de verificación para cualquier tipo de dispositivo para el que no desee configurar el perfil.
9. Realice las acciones siguientes:
   a) Haga clic en la pestaña de un tipo de dispositivo.
   b) Configure los valores adecuados para cada configuración del perfil para que coincida con la configuración del servicio SCEP del entorno de la empresa.
10. Repita el paso 8 para cada tipo de dispositivo en la empresa.
11. Haga clic en **Agregar**.

Después de terminar: Si los dispositivos utilizan el certificado de cliente para autenticarse en una red Wi-Fi de trabajo, VPN de trabajo o servidor de correo, asociar el perfil SCEP con una Wi-Fi, una VPN, o un perfil de correo.

Conceptos relacionados

Ajustes del perfil SCEP

Envío del mismo certificado de cliente a varios dispositivos

Puede utilizar perfiles de certificados compartidos para enviar certificados de cliente a los dispositivos iOS, macOS y Android.

Los perfiles de certificado compartido envían el mismo par de claves a cada usuario al que se le ha asignado el perfil. Debe utilizar perfiles de certificado compartido solo si desea permitir a más de un usuario compartir un certificado de cliente.

macOS aplica perfiles a las cuentas de usuario o los dispositivos. Puede configurar un perfil de certificado compartido para aplicarlo a una u otra opción.

Tareas relacionadas

Adición de un certificado de cliente a una cuenta de usuario

Creación de un perfil de certificado compartido

Antes de empezar: Debe obtener el archivo del certificado de cliente que desea enviar a los dispositivos. El archivo del certificado debe tener una extensión de nombre de archivo .pfx o p12.

1. En la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Certificados > Certificado compartido**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil. Cada perfil de certificado debe tener un nombre único. Algunos nombres (por ejemplo, ca_1) están reservados.
5. En el campo **Contraseña**, escriba una contraseña para el perfil de certificado compartido.
6. En el campo **Archivo de certificado**, haga clic en **Examinar** para ubicar el archivo de certificado.
7. En la pestaña **macOS**, en la lista desplegable **Aplicar perfil a**, seleccione **Usuario** o **Dispositivo**.
8. Haga clic en **Agregar**.

Tareas relacionadas

Asignación de un perfil o una política de TI a un grupo de usuarios

Asignar un perfil o una política de TI a una cuenta de usuario

Especificar el certificado utilizado por una aplicación

Para los dispositivos que utilizan Android 7.0 y posteriores, puede utilizar un perfil de asignación de certificados para especificar los certificados de cliente que utilizan las aplicaciones. El perfil de asignación de certificados no es compatible con las aplicaciones de BlackBerry Dynamics.

Los perfiles de asignación de certificados le permiten especificar los certificados que utilizan las aplicaciones de Android. Puede disponer que una aplicación utilice un certificado enviado al dispositivo mediante SCEP, credenciales de usuario o un perfil de certificado compartido. Puede utilizar un certificado con una o varias de las aplicaciones gestionadas, o todas. También puede especificar si una aplicación utiliza un certificado cada vez que se le solicita o únicamente para las conexiones a un URI determinado.

Se pueden especificar varias asignaciones de certificados en un mismo perfil. Solo se puede asignar un perfil de asignación de certificados a un usuario.

Create a certificate mapping profile

Before you begin: Create any SCEP, user credential, or shared certificate profiles required to send certificates to devices and assign the profiles to users or groups.

1. On the menu bar, click **Policies and Profiles**.
2. Click Certificates > Certificate mapping.
3. Click +.
4. Type a name and description for the profile. Each certificate profile must have a unique name.
5. In the mapping table, click +.
6. Under **Destination URI**, select one of the following options:
   - Select **None** if the app won't use the certificate to authenticate a connection with a resource.
   - Select **Any** if the app can use the certificate to authenticate a connection with any resource.
   - Select **Specified host:port** and type the host and port if the app can use the certificate to authenticate with a specific resource.
7. Under **App certificate**, perform one of the following actions:
   - To specify that the app must use a certificate sent to the device by another profile, select **Selected certificate** and select the profile name from the drop-down list.
   - To specify that the app must use a certificate sent to the device by a third-party source, select **Certificate alias** and type the alias for the certificate. If you do not know the alias, consult the documentation or administrator for the certificate provider.
   - To specify that the app must use a certificate sent to the device by another profile, select **Selected certificate** and select the profile name from the drop-down list.
8. Under **Allowed apps for destination URI**, perform one of the following actions:
   - To allow any managed app to request the specified certificate, select **Any apps in workspace**.
   - To allow only specified apps to request the certificate, select **Specified apps** and click + to specify one or more apps.
9. If necessary, repeat steps 5 to 8 to add to additional mappings to the profile.
10. Click **Add**.

After you finish:

- Assign the profile to user accounts and user groups.
- If necessary, rank profiles.

Políticas, estándares y conformidad de dispositivos

Puede utilizar políticas de TI y perfiles para aplicar algunos estándares para los dispositivos de la empresa. Una política de TI es un conjunto de reglas que controla las características y la funcionalidad de los dispositivos. Diferentes perfiles son compatibles con configuraciones particulares tales como el comportamiento de la aplicación BlackBerry Dynamics, las reglas de cumplimiento, las restricciones de contenido web o las de aplicaciones. Puede especificar la configuración de los dispositivos con BlackBerry 10, iOS, Android y Windows en la misma política de TI o el mismo perfil y, a continuación, asignar la política de TI o el perfil a las cuentas de usuario, a los grupos de usuarios o a los grupos de dispositivos.

Pasos para configurar las políticas y los estándares de la empresa para dispositivos

Al configurar las políticas y los estándares de la empresa para dispositivos, debe realizar las acciones siguientes:

Paso	Acción
1	Revise la política de TI predeterminada y, si es necesario, realice actualizaciones.
2	Opcionalmente, cree políticas de TI personalizadas.
3	Cree perfiles para aplicar algunos estándares en los dispositivos. Por ejemplo, crear un perfil de cumplimiento, un perfil de contenido web o un perfil de aviso de la empresa.
4	Si es necesario, clasificar las políticas de TI y los perfiles de clasificación.
5	Asigne políticas de TI y perfiles a las cuentas de usuario, a los grupos de usuarios o a los grupos de dispositivos.

Gestión de dispositivos con políticas de TI

Puede utilizar las políticas de TI para gestionar la seguridad y el comportamiento de los dispositivos en su empresa. Una política de TI es un conjunto de reglas que controla las características y la funcionalidad de los dispositivos. Puede configurar las reglas de los dispositivos con BlackBerry 10,iOS,macOS,Android y Windows en la misma política de TI. El SO del dispositivo determina la lista de características que se pueden controlar mediante políticas de TI y el tipo de activación del dispositivo determina qué reglas de una política de TI se aplican a un dispositivo concreto. Los dispositivos ignoran las reglas de la política de TI que no se les aplican.

BlackBerry UEM incluye una política de TI predeterminada con reglas preconfiguradas para cada tipo de dispositivo. Si no se asigna ninguna política de TI a una cuenta de usuario, a un grupo de usuarios al que pertenece el usuario o a un grupo de dispositivos a los que pertenecen los dispositivos del usuario, BlackBerry UEM envía la política de TI predeterminada a los dispositivos del usuario. BlackBerry UEM envía automáticamente una política de TI a un dispositivo cuando el usuario lo activa, cuando se actualiza una política de TI asignada o cuando una política de TI diferente está asignada a una cuenta de usuario o de dispositivo.

BlackBerry UEM se sincroniza diariamente con BlackBerry Infrastructure a través del puerto 3101 para determinar si cualquier información de política de TI actualizada está disponible. Si la información de política de TI actualizada está disponible, BlackBerry UEM la recupera y guarda las actualizaciones en la base de datos de BlackBerry UEM. A los administradores con los permisos "Ver políticas de TI" y "Crear y editar políticas de TI" se les notifica acerca de la actualización cuando inician sesión.

Para obtener más información acerca de las reglas de política de TI para cada tipo de dispositivo, descargue la hoja de cálculo de referencia de políticas.

Restricción o autorización de las capacidades del dispositivo

Al configurar las reglas de políticas de TI, puede restringir o permitir las capacidades del dispositivo. Las reglas de políticas de TI disponibles para cada tipo de dispositivo están determinadas por el sistema operativo del dispositivo y por su versión, y por el tipo de activación del dispositivo. Por ejemplo, dependiendo del tipo de dispositivo y de activación, puede utilizar reglas de políticas de TI para:

- Imponer requisitos de contraseña para el dispositivo o el espacio de trabajo en un dispositivo
- Impedir que los usuarios utilicen funciones del dispositivo, como la cámara
- Controlar conexiones que utilizan la tecnología inalámbrica Bluetooth
- Controlar la disponibilidad de algunas aplicaciones
- Requerir cifrado y otras características de seguridad

Dependiendo del tipo de activación del dispositivo, puede utilizar las reglas de política de TI para controlar todo el dispositivo, solo el espacio de trabajo en un dispositivo, o ambos.

En los dispositivos con Android 8.0 y versiones posteriores, puede crear un mensaje de ayuda del dispositivo que se muestra en el dispositivo cuando algunas funciones cuando se desactivan debido a reglas de políticas de TI.

Para obtener más información acerca de las reglas de política de TI para cada tipo de dispositivo, descargue la hoja de cálculo de referencia de políticas.

Establecimiento de los requisitos de la contraseña del dispositivo

Puede utilizar las reglas de políticas de TI para configurar los requisitos de la contraseña de los dispositivos. Puede configurar los requisitos sobre la longitud y la complejidad de la contraseña, la caducidad de esta y el resultado del seguimiento de contraseñas incorrectas. Los temas siguientes explican las reglas de las contraseñas que se aplican a los distintos dispositivos y a los tipos de activación.

Para obtener más información acerca de las reglas de políticas de TI,descargue la hoja de cálculo de referencia de políticas.

Establecimiento de los requisitos de la contraseña de BlackBerry 10

En los dispositivos con BlackBerry 10, las reglas de las contraseñas afectan a la contraseña del espacio de trabajo. Los dispositivos "Solo espacio de trabajo" deben contar con una contraseña y puede establecer los requisitos para esta.

Puede elegir si los dispositivos "Trabajo y personal - Empresa " y "Trabajo y personal - Regulado" deben contar con una contraseña del espacio de trabajo. Si requiere contraseñas del espacio de trabajo, puede establecer los requisitos mínimos para la contraseña, especificar si el dispositivo también debe tener una contraseña y especificar si las contraseñas del espacio de trabajo y del dispositivo pueden o deben ser iguales.

Regla	Detalles
Contraseña requerida para el espacio de trabajo	Especifique si los dispositivos "Trabajo y personal - Empresa" y "Trabajo y personal - Regulado" requieren una contraseña del espacio de trabajo. Los dispositivos "Solo espacio de trabajo" deben tener una contraseña.
Longitud mínima de la contraseña:	Especifique la longitud mínima de la contraseña del espacio de trabajo. La contraseña debe tener al menos 4 caracteres.
Complejidad mínima de la contraseña	Especifique la complejidad mínima de la contraseña del espacio de trabajo. Puede elegir una de las siguientes opciones: • Sin restricciones • Mínimo de 1 letra y 1 número • Mínimo de 1 letra, 1 número y 1 carácter especial • Mínimo de 1 letra mayúscula, 1 letra minúscula, 1 número y 1 carácter especial • Mínimo de 1 letra mayúscula, 1 letra minúscula y 1 número
Tiempo de espera de seguridad	Especifique el periodo de inactividad del usuario que debe transcurrir antes de que se bloquee el espacio de trabajo.
Máximo de intentos de introducción de la contraseña	Especifique el número de veces que un usuario puede introducir una contraseña incorrecta antes de que se eliminen los datos del espacio de trabajo. En los dispositivos "Trabajo y personal - Empresa" y "Trabajo y personal - Regulado", si el espacio de trabajo y el dispositivo tienen la misma contraseña, el dispositivo se borrará.
Historial máximo de contraseñas	Especifique el número de contraseñas anteriores que el dispositivo debe comprobar para evitar que un usuario vuelva a utilizar una contraseña del espacio de trabajo. Si se establece en 0, el dispositivo no comprueba las contraseñas anteriores.
Tiempo máximo de validez de la contraseña	Especifique el número máximo de días que puede utilizarse la contraseña del espacio de trabajo. Si se establece en 0, la contraseña no caduca.
Requerir contraseña para todo el dispositivo	Especifique si los dispositivos "Trabajo y personal - Empresa" y "Trabajo y personal - Regulado" requieren una contraseña para el dispositivo, así como para el espacio de trabajo.
Definir el espacio de trabajo y el comportamiento de la contraseña del dispositivo	Especifique si la contraseña del espacio de trabajo y la contraseña del dispositivo deben ser diferentes, deben ser iguales o si el usuario puede elegir si las contraseñas son iguales.

Para obtener más información acerca de las reglas de la contraseña de la política de TI,descargue la hoja de cálculo de referencia de políticas.

Establecimiento de los requisitos de la contraseña de iOS

Puede elegir si los dispositivos iOS deben tener una contraseña. Si se requiere una contraseña, puede establecer los requisitos para esta.

Nota: Los dispositivos iOS y algunas reglas para la contraseña del dispositivo utilizan el término "código de acceso". Ambos, tanto "contraseña" como "código de acceso", tienen el mismo significado.

Regla	Descripción
Se requiere contraseña para el dispositivo	Especifique si el usuario debe establecer una contraseña para el dispositivo.
Permitir valor simple	Especifique si la contraseña puede contener caracteres repetidos o secuenciales, como DEFG o 3333.
Requerir valor alfanumérico	Especifique si la contraseña deberá contener letras y números.
Longitud mínima del código de acceso	Especifique la longitud mínima de la contraseña. Si introduce un valor que es menor que el mínimo requerido por el dispositivo iOS, se utiliza dicho mínimo.
Número mínimo de caracteres complejos	Especifique el número mínimo de caracteres no alfanuméricos que debe contener la contraseña del dispositivo.
Periodo máximo de validez del código de acceso	Especifique el número máximo de días que puede utilizarse la contraseña.
Bloqueo automático máximo	Especifique el valor máximo que un usuario puede establecer para el tiempo de bloqueo automático, que se corresponde con el número de minutos de inactividad del usuario que deben transcurrir antes de que el dispositivo se bloquee. Si se establece en "Ninguno", todos los valores compatibles estarán disponibles en el dispositivo. Si el valor seleccionado se encuentra fuera del intervalo compatible con el dispositivo, el dispositivo utilizará el valor más cercano compatible.
Historial de códigos de acceso	Especifique el número de contraseñas anteriores que el dispositivo debe comprobar para evitar que un usuario vuelva a utilizar una contraseña reciente.
Periodo máximo de gracia para el bloqueo del dispositivo	Especifique el valor máximo que un usuario puede establecer para el periodo de gracia para el bloqueo del dispositivo, que se corresponde con la cantidad de tiempo que un dispositivo puede permanecer bloqueado antes de que se requiera una contraseña para desbloquearlo. Si se establece en "Ninguno", todos los valores estarán disponibles en el dispositivo. Si se establece en "Inmediatamente", la contraseña se necesita inmediatamente después de que el dispositivo se bloquee.
Número máximo de intentos de contraseña fallidos	Especifique el número de veces que un usuario puede introducir una contraseña incorrecta antes de que se eliminen los datos del dispositivo.
Permitir cambios de contraseña (solo con supervisión)	Especifique si un usuario puede agregar, cambiar o eliminar la contraseña.

Para obtener más información acerca de las reglas de la contraseña de la política de TI,descargue la hoja de cálculo de referencia de políticas.

Establecimiento de los requisitos de la contraseña de macOS

Puede elegir si las reglas de contraseña para dispositivos con macOS se aplican al dispositivo o al usuario y si es necesaria una contraseña. Si se requiere una contraseña, puede establecer los requisitos para esta.

Regla	Descripción
Objetivo de las reglas de políticas de TI	Esta regla especifica si las reglas de políticas de TI para la contraseña deben aplicarse únicamente a la cuenta del usuario asignado o a la totalidad del dispositivo.
Se requiere contraseña para el dispositivo	Especifique si el usuario debe establecer una contraseña para el dispositivo.
Permitir contraseña sencilla	Especifique si la contraseña puede contener caracteres repetidos o secuenciales, como DEFG o 3333.
Requerir valor alfanumérico	Especifique si la contraseña deberá contener letras y números.
Longitud mínima de la contraseña:	Especifique la longitud mínima de la contraseña.
Número mínimo de caracteres complejos	Especifique el número mínimo de caracteres no alfanuméricos que debe contener la contraseña del dispositivo.
Tiempo máximo de validez de la contraseña	Especifique un número de días máximo durante el cual se pueda utilizar la contraseña antes de caducar y que el usuario deba establecer una contraseña nueva.
Bloqueo automático máximo	Especifique el número máximo de minutos de inactividad del usuario que debe transcurrir antes de que un dispositivo se bloquee. Si se ha configurado en "Ninguno", el usuario puede seleccionar cualquier valor.
Historial de contraseñas	Especifique el número máximo de contraseñas anteriores que el dispositivo debe comprobar para evitar que un usuario vuelva a utilizar una contraseña.
Periodo máximo de gracia para el bloqueo del dispositivo	Especifique el valor máximo que un usuario puede establecer para el periodo de gracia para el bloqueo del dispositivo, que se corresponde con la cantidad de tiempo que un dispositivo puede permanecer bloqueado antes de que se requiera una contraseña para desbloquearlo.
Número máximo de intentos de contraseña fallidos	Especifique el número de veces que un usuario puede introducir una contraseña incorrecta antes de que se eliminen los datos del dispositivo.

Para obtener más información acerca de las reglas de la contraseña de la política de TI, descargue la hoja de cálculo de referencia de políticas.

Establecimiento de los requisitos de la contraseña de Android

Hay cuatro grupos de reglas de políticas de TI en las contraseñas Android. El grupo de reglas que se utilice depende del tipo de activación del dispositivo y si se van a establecer requisitos para la contraseña del dispositivo o para la contraseña del espacio de trabajo.

Tipo de activación	Compatibilidad con las reglas para la contraseña
Controles de MDM	Utilice las reglas para la contraseña de SO nativo para establecer los requisitos de la contraseña del dispositivo. El dispositivo ignora el resto de las reglas para la contraseña. Utilice un perfil de conformidad para hacer que se cumplan los requisitos relacionados con las contraseñas.
Solo espacio de trabajo Solo espacio de trabajo (Premium)	Utilice las reglas para la contraseña de SO nativo para establecer los requisitos de la contraseña del dispositivo. Puesto que el dispositivo solo cuenta con un espacio de trabajo, la contraseña también es la contraseña del espacio de trabajo. El dispositivo ignora el resto de las reglas para la contraseña. Utilice un perfil de conformidad para hacer que se cumplan los requisitos relacionados con las contraseñas.
Trabajo y personal: privacidad de usuario Trabajo y personal: privacidad de usuario (Premium)	Utilice las reglas para la contraseña de SO nativo para establecer los requisitos de la contraseña del dispositivo. Utilice las reglas para la contraseña de los perfiles de trabajo de Android para establecer los requisitos de la contraseña del espacio de trabajo. Para dispositivos BlackBerry con Android, puede forzar el espacio de trabajo y las contraseñas de los dispositivos para que sean diferentes. El dispositivo ignora el resto de las reglas para la contraseña. Utilice un perfil de conformidad para hacer que se cumplan los requisitos relacionados con las contraseñas.
Controles de MDM (KNOX MDM)	Utilice las reglas para la contraseña de KNOX MDM para establecer los requisitos de la contraseña del dispositivo. El dispositivo ignora el resto de las reglas para la contraseña. Utilice un perfil de conformidad para hacer que se cumplan los requisitos relacionados con las contraseñas.
Solo espacio de trabajo (Samsung KNOX)	Utilice las reglas para la contraseña KNOX Premium - Workspace para establecer los requisitos de la contraseña del espacio de trabajo. El dispositivo ignora el resto de las reglas para la contraseña. Utilice un perfil de conformidad para hacer que se cumplan los requisitos relacionados con las contraseñas.

Tipo de activación	Compatibilidad con las reglas para la contraseña
Trabajo y personal: control total (Samsung KNOX)	Utilice las reglas para la contraseña de KNOX MDM para establecer los requisitos de la contraseña del dispositivo. Utilice las reglas para la contraseña KNOX Premium - Workspace para establecer los requisitos de la contraseña del espacio de trabajo. El dispositivo ignora el resto de las reglas para la contraseña. Utilice un perfil de conformidad para hacer que se cumplan los requisitos relacionados con las contraseñas.
Trabajo y personal: privacidad de usuario (Samsung KNOX)	No tiene ningún control sobre la contraseña del dispositivo. Utilice las reglas para la contraseña KNOX Premium - Workspace para establecer los requisitos de la contraseña del espacio de trabajo. El dispositivo ignora el resto de las reglas para la contraseña. Utilice un perfil de conformidad para hacer que se cumplan los requisitos relacionados con las contraseñas.

Android: reglas para la contraseña del SO nativo

Las reglas para la contraseña del SO Nativo establecen los requisitos de la contraseña del dispositivo para los dispositivos con los siguientes tipos de activación:

- Controles de MDM (sin Samsung KNOX)
- Solo espacio de trabajo
- Solo espacio de trabajo (Premium)
- Trabajo y personal: privacidad de usuario
- Trabajo y personal: privacidad de usuario (Premium)

Regla	Descripción
Requisitos de la contraseña	Especifique los requisitos mínimos de la contraseña. Puede elegir una de las siguientes opciones: • Sin especificar: no se requiere contraseña • Algunos: el usuario deberá establecer una contraseña pero no habrá requisitos relacionados con la longitud o la calidad • Numérica: la contraseña deberá incluir al menos un número • Alfabética: la contraseña deberá incluir al menos una letra • Alfanumérica: la contraseña deberá incluir al menos una letra y un número • Complejos: permite establecer requisitos específicos para los diferentes tipos de caracteres

Regla	Descripción
Número máximo de intentos de contraseña fallidos	Especifique el número de veces que un usuario puede introducir una contraseña incorrecta antes de que el dispositivo se desactive o se eliminen sus datos. Se eliminan los dispositivos con el tipo de activación "Controles de MDM". Se desactivarán los dispositivos con los tipos de activación "Trabajo y personal: privacidad de usuario " y "Trabajo y personal: privacidad de usuario (Premium)" y se eliminará el perfil de trabajo.
Bloqueo de tiempo de inactividad máximo	Especifique cuántos minutos de inactividad del usuario deben transcurrir antes de que el dispositivo o el espacio de trabajo se bloqueen. Esta regla se ignora si no se necesita contraseña.
Tiempo de espera de caducidad de la contraseña	Especifique la cantidad máxima de tiempo que puede utilizarse la contraseña. Una vez transcurrida la cantidad de tiempo especificada, el usuario deberá establecer una nueva contraseña. Si se establece en 0, la contraseña no caduca.
Restricción del historial de contraseñas	Especifique el número máximo de contraseñas anteriores que el dispositivo debe comprobar para evitar que un usuario vuelva a utilizar una contraseña numérica, alfabética, alfanumérica o compleja reciente. Si se establece en 0, el dispositivo no comprueba las contraseñas anteriores.
Longitud mínima de la contraseña:	Especifique el número mínimo de caracteres necesarios en una contraseña numérica, alfabética, alfanumérica o compleja.
Número mínimo de letras mayúsculas requerido en la contraseña	Especifique el número mínimo de letras mayúsculas que debe contener una contraseña compleja.
Número mínimo de letras minúsculas requerido en la contraseña	Especifique el número mínimo de letras minúsculas que debe contener una contraseña compleja.
Número mínimo de letras requerido en la contraseña	Especifique el número mínimo de letras que debe contener una contraseña compleja.
Número mínimo de caracteres no alfabéticos en la contraseña	Especifique el número mínimo de caracteres no alfabéticos (números o símbolos) que debe contener una contraseña compleja.
Número mínimo de dígitos numéricos requerido en la contraseña	Especifique el número mínimo de números que debe contener una contraseña compleja.
Número mínimo de símbolos requerido en la contraseña	Especifique el número mínimo de caracteres complejos que debe contener una contraseña compleja.

Para obtener más información acerca de las reglas de la contraseña de la política de TI, descargue la hoja de cálculo de referencia de políticas.

Android: reglas para las contraseñas de los perfiles de trabajo de Android

Las reglas para las contraseñas de los perfiles de trabajo de Android establecen los requisitos de la contraseña del espacio de trabajo para los dispositivos con los siguientes tipos de activación:

- Trabajo y personal: privacidad de usuario
- Trabajo y personal: privacidad de usuario (Premium)

Regla	Descripción
Requisitos de la contraseña	Especifique los requisitos mínimos de la contraseña del espacio de trabajo. Puede elegir una de las siguientes opciones: • Sin especificar: no se requiere contraseña • Algunos: el usuario deberá establecer una contraseña pero no habrá requisitos relacionados con la longitud o la calidad • Numérica: la contraseña deberá incluir al menos un número • Alfabética: la contraseña deberá incluir al menos una letra • Alfanumérica: la contraseña deberá incluir al menos una letra y un número • Complejos: permite establecer requisitos específicos para los diferentes tipos de caracteres • Complejos, numérica: la contraseña debe contener caracteres numéricos con secuencias no repetidas (4444) ni ordenadas (1234, 4321, 2468). • Parámetros biométricos débiles: la contraseña permite la tecnología de reconocimiento biométrico de seguridad baja. Para dispositivos BlackBerry alimentados por Android, puede forzar el espacio de trabajo y las contraseñas de los dispositivos para que sean diferentes mediante la regla "Forzar el espacio de trabajo y las contraseñas de los dispositivos para que sean diferentes" de los dispositivos BlackBerry.
Número máximo de intentos de contraseña fallidos	Especifique el número de veces que un usuario puede introducir una contraseña incorrecta del espacio de trabajo para que se desactive el dispositivo y el perfil de trabajo se elimine.
Bloqueo de tiempo de inactividad máximo	Especifique cuántos minutos de inactividad del usuario deben transcurrir para que el dispositivo y el espacio de trabajo se bloqueen. Si configura esta regla y la regla "Bloqueo de tiempo de inactividad máximo" del SO nativo, el dispositivo y el espacio de trabajo se bloquean cuando el contador llega a su fin.
Tiempo de espera de caducidad de la contraseña	Especifique la cantidad máxima de tiempo que puede utilizarse la contraseña del espacio de trabajo. Una vez transcurrida la cantidad de tiempo especificada, el usuario deberá establecer una nueva contraseña del espacio de trabajo. Si se establece en 0, la contraseña no caduca.
Restricción del historial de contraseñas	Especifique el número máximo de contraseñas anteriores del espacio de trabajo que el dispositivo debe comprobar para evitar que un usuario vuelva a utilizar una contraseña numérica, alfabética, alfanumérica o compleja reciente. Si se establece en 0, el dispositivo no comprueba las contraseñas anteriores.
Longitud mínima de la contraseña:	Especifique el número mínimo de caracteres necesarios en una contraseña del espacio de trabajo numérica, alfabética, alfanumérica o compleja.

Regla	Descripción
Número mínimo de letras mayúsculas requerido en la contraseña	Especifique el número mínimo de letras en mayúscula que debe contener la contraseña compleja del espacio de trabajo.
Número mínimo de letras minúsculas requerido en la contraseña	Especifique el número mínimo de letras en minúscula que debe contener la contraseña compleja del espacio de trabajo.
Número mínimo de letras requerido en la contraseña	Especifique el número mínimo de letras que debe contener la contraseña compleja del espacio de trabajo.
Número mínimo de caracteres no alfabéticos en la contraseña	Especifique el número mínimo de caracteres no alfabéticos (números o símbolos) que debe contener una contraseña compleja del espacio de trabajo.
Número mínimo de dígitos numéricos requerido en la contraseña	Especifique el número mínimo de números que debe contener la contraseña compleja del espacio de trabajo.
Número mínimo de símbolos requerido en la contraseña	Especifique el número mínimo de caracteres no alfanuméricos que debe contener una contraseña compleja del espacio de trabajo.

Para obtener más información acerca de las reglas de la contraseña de la política de TI, descargue la hoja de cálculo de referencia de políticas.

Android: reglas para la contraseña de KNOX MDM

Las reglas para la contraseña de KNOX MDM establecen los requisitos de la contraseña del dispositivo para los dispositivos con los siguientes tipos de activación:

- Controles de MDM (KNOX MDM)
- Trabajo y personal: control total (Samsung KNOX)

Los dispositivos con estos tipos de activación deben tener una contraseña para el dispositivo.

Regla	Descripción
Requisitos de la contraseña	Especifique los requisitos mínimos de la contraseña. Puede elegir una de las siguientes opciones: • Numérica: la contraseña deberá incluir al menos un número • Alfabética: la contraseña deberá incluir al menos una letra • Alfanumérica: la contraseña deberá incluir al menos una letra y un número • Complejos: permite establecer requisitos específicos para los diferentes tipos de caracteres

Regla	Descripción
Longitud mínima de la contraseña:	Especifique la longitud mínima de la contraseña. La contraseña debe tener al menos 4 caracteres.
Número mínimo de letras minúsculas requerido en la contraseña	Especifique el número mínimo de letras minúsculas que debe contener una contraseña compleja.
Número mínimo de letras mayúsculas requerido en la contraseña	Especifique el número mínimo de letras mayúsculas que debe contener una contraseña compleja.
Número mínimo de caracteres complejos requerido en la contraseña	Especifique el número mínimo de caracteres complejos (por ejemplo, números y símbolos) que debe contener una contraseña compleja. Si establece este valor en 1, entonces se requerirá al menos un número. Si establece un valor superior a 1, se requerirán al menos un número y un símbolo.
Longitud máxima de la secuencia de caracteres	Especifique la longitud máxima de una secuencia alfabética permitida en una contraseña alfanumérica o compleja. Por ejemplo, si la longitud de la secuencia alfabética se establece en 5, la secuencia "abcde" estará permitida, pero no la secuencia "abcdef". Si se establece en 0, no habrá restricciones para las secuencias alfabéticas.
Bloqueo de tiempo de inactividad máximo	Especifique el periodo de inactividad del usuario que debe transcurrir antes de que el dispositivo se bloquee (bloqueo protegido con clave). Si el dispositivo se gestiona por varias soluciones EMM, este utilizará el valor más bajo como periodo de inactividad. Si el dispositivo utiliza una contraseña, el usuario deberá proporcionar la contraseña para desbloquear el dispositivo. Si se establece en 0, el dispositivo no contará con un tiempo de espera de inactividad.
Número máximo de intentos de contraseña fallidos	Especifique el número de veces que un usuario puede introducir una contraseña incorrecta antes de que se eliminen los datos del dispositivo.
Restricción del historial de contraseñas	Especifique el número máximo de contraseñas anteriores que el dispositivo debe comprobar para evitar que un usuario vuelva a utilizar una contraseña reciente. Si se establece en 0, el dispositivo no comprueba las contraseñas anteriores.
Tiempo de espera de caducidad de la contraseña	Especifique la cantidad máxima de tiempo que puede utilizarse la contraseña del dispositivo. Una vez transcurrida la cantidad de tiempo especificada, la contraseña caducará y el usuario deberá establecer una nueva contraseña. Si se establece en 0, la contraseña no caduca.
Permitir visibilidad de la contraseña	Especifique si desea que la contraseña del dispositivo pueda ser visible cuando el usuario la escriba. Si no se selecciona esta regla, los usuarios y las aplicaciones de terceros no podrán modificar la configuración de visibilidad.
Permitir la autenticación mediante huella digital	Especifique si el usuario puede usar autenticación de huella digital para el dispositivo.

Para obtener más información acerca de las reglas de la contraseña de la política de TI,descargue la hoja de cálculo de referencia de políticas.

Android: reglas para la contraseña de KNOX Premium - Workspace

Las reglas para la contraseña de KNOX Premium - Workspace establecen los requisitos de la contraseña del espacio de trabajo para los dispositivos con los siguientes tipos de activación:

- Solo espacio de trabajo (Samsung KNOX)
- Trabajo y personal: control total (Samsung KNOX)
- Trabajo y personal: privacidad de usuario (Samsung KNOX)

Los dispositivos con estos tipos de activación deben tener una contraseña del espacio de trabajo.

Regla	Descripción
Requisitos de la contraseña	Especifique los requisitos mínimos de la contraseña. Puede elegir una de las siguientes opciones: • Numérica: la contraseña deberá incluir al menos un número • "Complejos, numérica": la contraseña deberá incluir al menos un número con secuencias no repetidas (4444) ni ordenadas (1234, 4321, 2468) • Alfabética: la contraseña deberá incluir al menos una letra • Alfanumérica: la contraseña deberá incluir al menos una letra y un número • Complejos: permite establecer requisitos específicos para los diferentes tipos de caracteres
Número mínimo de letras minúsculas requerido en la contraseña	Especifique el número mínimo de letras minúsculas que debe contener una contraseña compleja.
Número mínimo de letras mayúsculas requerido en la contraseña	Especifique el número mínimo de letras mayúsculas que debe contener una contraseña compleja.
Número mínimo de caracteres complejos requerido en la contraseña	Especifique el número mínimo de caracteres complejos (por ejemplo, números y símbolos) que debe contener una contraseña compleja. Al menos se requieren tres caracteres complejos, que incluyan al menos un número y un símbolo.
Longitud máxima de la secuencia de caracteres	Especifique la longitud máxima de una secuencia alfabética permitida en una contraseña alfanumérica o compleja. Por ejemplo, si la longitud de la secuencia alfabética se establece en 5, la secuencia "abcde" estará permitida, pero no la secuencia "abcdef". Si se establece en 0, no habrá restricciones para las secuencias alfabéticas.
Longitud mínima de la contraseña:	Especifique la longitud mínima de la contraseña. Si introduce un valor que es menor que el mínimo requerido por KNOX Workspace, se utiliza el mínimo KNOX Workspace.
Bloqueo de tiempo de inactividad máximo	Especifique el periodo de inactividad del usuario en el espacio de trabajo que debe transcurrir antes de que se bloquee el espacio de trabajo. Si se establece en 0, el espacio de trabajo no contará con un tiempo de espera de inactividad.

Regla	Descripción
Número máximo de intentos de contraseña fallidos	Especifique el número de veces que un usuario puede introducir una contraseña incorrecta antes de que se eliminen los datos del espacio de trabajo. Si se establece en 0, no habrá restricciones en el número de veces que un usuario puede introducir una contraseña incorrecta.
Restricción del historial de contraseñas	Especifique el número máximo de contraseñas anteriores que el dispositivo debe comprobar para evitar que un usuario vuelva a utilizar una contraseña reciente. Si se establece en 0, el dispositivo no comprueba las contraseñas anteriores.
Tiempo de espera de caducidad de la contraseña	Especifique el número máximo de días que puede utilizarse la contraseña. Una vez transcurrido el número de días especificado, la contraseña caducará y el usuario deberá establecer una nueva contraseña. Si se establece en 0, la contraseña no caduca.
Número mínimo de caracteres modificados para las nuevas contraseñas	Especifique el número mínimo de caracteres modificados que debe incluir una nueva contraseña en comparación con la contraseña anterior. Si se establece en 0, no se aplican restricciones.
Permitir personalización de la clave de bloqueo	Especifique si un dispositivo puede utilizar la personalización de la clave de bloqueo, como los agentes de confianza. Si no se selecciona esta regla, la personalización de la clave de bloqueo se desactivará.
Permitir agentes de confianza de la clave de bloqueo	Especifique si un usuario puede mantener el espacio de trabajo desbloqueado durante 2 horas después del tiempo de espera máximo de inactividad. Si no establece un valor para el tiempo de inactividad, el usuario podrá realizar esta acción de forma predeterminada.
Permitir visibilidad de la contraseña	Especifique si desea que la contraseña del dispositivo pueda ser visible cuando el usuario la escriba. Si no se selecciona esta regla, los usuarios y las aplicaciones de terceros no podrán modificar la configuración de visibilidad.
Ejecutar autenticación de dos factores	Especifique si un usuario debe utilizar la autenticación en dos fases para acceder al espacio de trabajo. Por ejemplo, puede utilizar esta regla si desea que el usuario se autentique utilizando una huella digital y una contraseña.
Permitir la autenticación mediante huella digital	Especifique si el usuario puede usar la autenticación mediante huella digital para acceder al espacio de trabajo.

Para obtener más información acerca de las reglas de la contraseña de la política de TI,descargue la hoja de cálculo de referencia de políticas.

Establecimiento de los requisitos de la contraseña de Windows

Puede elegir si los dispositivos Windows deben tener una contraseña. Si se requiere una contraseña, puede establecer los requisitos para esta.

Regla	Descripción
Se requiere contraseña para el dispositivo	Especifique si el usuario debe establecer una contraseña para el dispositivo.
Permitir contraseña sencilla	Especifique si la contraseña puede contener caracteres repetidos o secuenciales, como DEFG o 3333.
Longitud mínima de la contraseña:	Especifique la longitud mínima de la contraseña. La contraseña debe tener al menos 4 caracteres.
Complejidad de la contraseña	Especifique la complejidad de la contraseña. Puede elegir las siguientes opciones: • Alfanumérica: la contraseña deberá contener letras y números • Numérica: la contraseña deberá contener solo números
Número mínimo de tipos de caracteres	Especifique el número mínimo de tipos de caracteres que debe contener una contraseña alfanumérica. Seleccione de entre las siguientes opciones: **1.** números necesarios **2.** números y letras en minúscula necesarios **3.** números, letras mayúsculas y letras minúsculas necesarios **4.** números, letras mayúsculas y letras minúsculas y caracteres especiales necesarios Los requisitos de caracteres de contraseña para equipos y tabletas con Windows 10 se determinan en función del tipo de cuenta de usuario, no de esta configuración.
Caducidad de la contraseña	Especifique el número máximo de días que puede utilizarse la contraseña. Si se establece en 0, la contraseña no caduca.
Historial de contraseñas	Especifique el número de contraseñas anteriores que el dispositivo debe comprobar para evitar que un usuario vuelva a utilizar una contraseña reciente. Si se establece en 0, el dispositivo no comprueba las contraseñas anteriores.
Número máximo de intentos de contraseña fallidos	Especifique el número de veces que un usuario puede introducir una contraseña incorrecta antes de que se eliminen los datos del dispositivo. Si se establece en 0, no se eliminarán los datos del dispositivo con independencia de las veces que el usuario haya introducido una contraseña incorrecta. Esta regla no se aplica a los dispositivos que permiten varias cuentas de usuario, incluyendo los equipos y tabletas con Windows 10.
Bloqueo de tiempo de inactividad máximo	Especifique el periodo de inactividad del usuario que debe transcurrir antes de que el dispositivo se bloquee. Si se establece en 0, el dispositivo no se bloquea automáticamente.
Permitir salir del estado inactivo sin contraseña	Especifique si un usuario debe escribir la contraseña una vez que termine el periodo de gracia de la inactividad. Si se selecciona esta regla, el usuario podrá establecer el temporizador del periodo de gracia de la contraseña en el dispositivo. Esta regla no se aplica a equipos y tabletas Windows 10.

Para obtener más información acerca de las reglas de la contraseña de la política de TI,descargue la hoja de cálculo de referencia de políticas.

¿Cómo elige BlackBerry UEM qué política de TI asignar?

BlackBerry UEM envía una sola política de TI a un dispositivo y utiliza reglas predefinidas para determinar la política de TI que se asigna a un usuario y a los dispositivos que el usuario activa.

Asignado a	Reglas
Cuenta de usuario (ver pestaña Resumen)	1. Una política de TI asignada directamente a una cuenta de usuario tiene prioridad sobre una política de TI asignada indirectamente por grupo de usuarios. 2. Si un usuario es miembro de varios grupos de usuarios que tienen políticas de TI diferentes, BlackBerry UEM asigna la política de TI con la clasificación más alta. 3. La política de TI predeterminada se asigna si no hay otra que esté asignada directamente a una cuenta de usuario o a través de la pertenencia a un grupo de usuarios.
Dispositivo (ver pestaña dispositivo)	De forma predeterminada, un dispositivo hereda la política de TI que BlackBerry UEM asigna al usuario que lo activa. Si un dispositivo pertenece a un grupo de dispositivos, se aplican las siguientes reglas: 1. Una política de TI asignada a un grupo de dispositivos tiene prioridad sobre la política de TI que BlackBerry UEM asigna a un grupo de usuarios. 2. Si un dispositivo es miembro de varios grupos de dispositivos que tienen políticas de TI diferentes, BlackBerry UEM asigna la política de TI con la clasificación más alta.

BlackBerry UEM puede tener que resolver los conflictos de las políticas de TI cuando se realicen alguna de las siguientes acciones:

- Asignación de una política de TI a una cuenta de usuario, a un grupo de usuarios o a un grupo de dispositivos
- Eliminación de una política de TI de una cuenta de usuario, a un grupo de usuarios o a un grupo de dispositivos
- Cambio de la clasificación de la política de TI
- Eliminación de una política de TI
- Cambiar la pertenencia a grupos de usuarios (cuentas de usuario y grupos anidados)
- Cambio de los atributos del dispositivo
- Cambio de la pertenencia a un grupo de dispositivos
- Eliminación de un grupo de usuarios o de un grupo de dispositivos

Tareas relacionadas

Clasificar políticas de TI

Creación y gestión de políticas de TI

Puede utilizar la política de TI predeterminada o crear políticas de TI personalizadas (por ejemplo, para especificar reglas de políticas de TI de diferentes grupos de usuarios o de dispositivos en la empresa). Si va a utilizar la política de TI predeterminada, debería revisarla y, si fuera necesario, actualizarla para asegurarse de que las reglas cumplan con los estándares de seguridad de la empresa.

Creación de una política de TI

1. En la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Política > Políticas de TI**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para la política de TI.
5. Haga clic en la pestaña para cada tipo de dispositivo en la empresa y configure los valores apropiados para las reglas de políticas de TI.

   Mantenga el ratón sobre el nombre de una regla para mostrar sugerencias de ayuda.
6. Haga clic en **Agregar**.

Después de terminar: Clasifique las políticas de TI.

Tareas relacionadas

Asignar un perfil o una política de TI a una cuenta de usuario
Asignación de un perfil o una política de TI a un grupo de usuarios

Copie una política de TI

Puede copiar las políticas de TI actuales para crear rápidamente políticas de TI personalizadas para los distintos grupos de la empresa.

1. En la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Política > Políticas de TI**.
3. Haga clic en el nombre de la política de TI que desea copiar.
4. Haga clic en .
5. Escriba un nombre y una descripción para la nueva política de TI.
6. Haga los cambios en las pestañas apropiadas para cada tipo de dispositivo.
7. Haga clic en **Agregar**.

Después de terminar: Clasifique las políticas de TI.

Tareas relacionadas

Asignar un perfil o una política de TI a una cuenta de usuario
Asignación de un perfil o una política de TI a un grupo de usuarios

Clasificar políticas de TI

La clasificación se utiliza para determinar la política de TI que BlackBerry UEM envía a un dispositivo en las situaciones siguientes:

- Un usuario es miembro de varios grupos de usuarios que tienen diferentes políticas de TI.
- Un dispositivo es miembro de varios grupos de dispositivos que tienen diferentes políticas de TI.

1. En la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Política > Políticas de TI**.
3. Haga clic en .
4. Utilice las flechas para mover las políticas de TI hacia arriba o hacia abajo en la clasificación.

5. Haga clic en **Guardar**.

Conceptos relacionados

¿Cómo elige BlackBerry UEM qué política de TI asignar?

Presentación de políticas de TI

Puede ver la siguiente información acerca de una política de TI:

- Reglas de políticas de TI específicas para cada tipo de dispositivo
- La lista y el número de cuentas de usuario a las que la política de TI está asignada (directa e indirectamente)
- La lista y el número de grupos de usuarios a los que la política de TI está asignada (directamente)

1. En la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Política > Políticas de TI**.
3. Haga clic en el nombre de la política de TI que desea ver.

Cambio de una política de TI

1. En la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Política > Políticas de TI**.
3. Haga clic en el nombre de la política de TI que desea cambiar.
4. Haga clic en .
5. Haga los cambios en las pestañas apropiadas para cada tipo de dispositivo.
6. Haga clic en **Guardar**.

Después de terminar: Si es necesario, cambie la clasificación de la política de TI.

Tareas relacionadas

Clasificar políticas de TI

Eliminación de una política de TI de las cuentas o de los grupos de usuarios

Si una política de TI se asigna directamente a las cuentas o los grupos de usuarios, puede eliminarla. Si a un grupo de usuarios se asigna directamente una política de TI, se podrá eliminar la política de TI o las cuentas de usuario del grupo. Al eliminar una política de TI de los grupos de usuarios, se eliminará la política de TI de cada usuario que pertenezca a los grupos seleccionados.

Nota: La política de TI predeterminada solo se puede eliminar de una cuenta de usuario si se ha asignado directamente al usuario.

1. En la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Política > Políticas de TI**.
3. Haga clic en el nombre de la política de TI que desea eliminar de las cuentas o grupos de usuarios.
4. Lleve a cabo una de las tareas siguientes:

Tarea	Pasos
Eliminar una política de TI de las cuentas de usuario	**a.** Haga clic en la pestaña **Asignación para usuarios**. **b.** Si es necesario, busque cuentas de usuario. **c.** Seleccione las cuentas de usuario de las que desea eliminar de la política de TI. **d.** Haga clic en .
Eliminar una política de TI de los grupos de usuarios	**a.** Haga clic en la pestaña **Asignación para grupos**. **b.** Si es necesario, busque grupos de usuarios. **c.** Seleccione los grupos de usuarios de los que desea eliminar la política de TI. **d.** Haga clic en .

Conceptos relacionados

¿Cómo elige BlackBerry UEM qué política de TI asignar?

Eliminación de una política de TI

No puede eliminar la política de TI predeterminada. Cuando se elimina una política de TI personalizada, BlackBerry UEM elimina la política de TI de los usuarios y dispositivos a los que está asignada.

1. En la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Política > Políticas de TI**.
3. Seleccione las casillas de verificación de las políticas de TI que desea eliminar.
4. Haga clic en .
5. Haga clic en **Eliminar**.

Conceptos relacionados

¿Cómo elige BlackBerry UEM qué política de TI asignar?

Exporte las políticas de TI

Puede exportar las políticas de TI a un archivo .xml para fines de auditoría.

Nota:

Los perfiles que están asociados a las políticas de TI no se exportan.

1. En la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Política > Políticas de TI**.
3. Seleccione las casillas de verificación de las políticas de TI que desea exportar.
4. Haga clic en .
5. Haga clic en **Siguiente**.
6. Haga clic en **Exportar**.

Control de las capacidades del dispositivo con BlackBerry OS mediante políticas de TI

Si el dominio de BlackBerry UEM admite los dispositivos con BlackBerry OS (de la versión 5.0 a la 7.1), puede utilizar las políticas de TI de BlackBerry OS para controlar y administrar los dispositivos con BlackBerry OS, BlackBerry Desktop Software y BlackBerry Web Desktop Manager en el entorno de la empresa.

Para obtener más información acerca de la creación o actualización de políticas de TI para dispositivos con BlackBerry OS, descargue la Guía de administración en help.blackberry.com/detectLang/bes5-for-exchange/.

Tareas relacionadas

Asignación de una política de TI de BlackBerry OS, un perfil o una configuración de software a un grupo de usuarios
Asignación de una política de TI de BlackBerry OS, un perfil o una configuración de software a una cuenta de usuario

Control de BlackBerry Dynamics en dispositivos de usuarios

El perfil BlackBerry Dynamics activa BlackBerry Dynamics para usuarios y establece los estándares de acceso, protección de datos y registro de las aplicaciones de BlackBerry Dynamics.

BlackBerry UEM incluye un perfil de BlackBerry Dynamics predeterminado con ajustes preconfigurados. Si no se asigna ningún perfil de BlackBerry Dynamics a una cuenta de usuario, a un grupo de usuarios al que pertenece el usuario o a un grupo de dispositivos a los que pertenecen los dispositivos del usuario, BlackBerry UEM envía el perfil de BlackBerry Dynamics predeterminado a los dispositivos del usuario. BlackBerry UEM envía automáticamente un perfil de BlackBerry Dynamics a un dispositivo cuando el usuario lo activa, cuando se actualiza un perfil de BlackBerry Dynamics asignado o cuando un perfil de BlackBerry Dynamics diferente está asignado a una cuenta de usuario o de dispositivo.

Se puede asignar el perfil de BlackBerry Dynamics a cuentas de usuarios, a grupos de usuarios y a grupos de dispositivos.

Referencia relacionada

Gestión de perfiles de conformidad de BlackBerry Dynamics

Creación de un perfil de BlackBerry Dynamics

1. En la barra de menú, haga clic en **Políticas y perfiles**.
2. Haga clic en **Política > BlackBerry Dynamics**
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil.
5. Configure los valores adecuados para la configuración del perfil. Para obtener más información acerca de la configuración de cada perfil, consulte Ajustes del perfil de BlackBerry Dynamics.
6. Haga clic en **Agregar**.

Después de terminar: Si fuera necesario, clasifique los perfiles.

Tareas relacionadas

Asignación de un perfil o una política de TI a un grupo de usuarios

Asignar un perfil o una política de TI a una cuenta de usuario

Referencia relacionada

Ajustes del perfil de BlackBerry Dynamics

Cumplimiento de las reglas de los dispositivos

Puede utilizar los perfiles de conformidad para alentar a los usuarios a seguir los estándares de la empresa en el uso de los dispositivos. Un perfil de cumplimiento define las condiciones del dispositivo que no son aceptables en la empresa. Por ejemplo, puede optar por no permitir los dispositivos que se han liberado o tienen acceso a la raíz, o bien aquellos que tienen una alerta de integridad debido al acceso no autorizado al sistema operativo.

Un perfil de cumplimiento especifica la información siguiente:

- Condiciones que podrían hacer que un dispositivo no cumpla los requisitos.
- Los mensajes de correo electrónico y las notificaciones de dispositivos que reciben los usuarios si infringen las condiciones de conformidad.
- Acciones que se realizan si los usuarios no corrigen el problema, que incluyen la limitación del acceso de un usuario a los recursos de la empresa, la eliminación de datos de trabajo del dispositivo o de todos los datos de dicho dispositivo.

En los dispositivos Samsung KNOX, puede agregar una lista de las aplicaciones restringidas a un perfil de cumplimiento. Sin embargo, BlackBerry UEM no impone el cumplimiento de las reglas de conformidad. En su lugar, la lista de aplicaciones restringidas se envía a los dispositivos y este es el que aplica el cumplimiento. No se podrán instalar aplicaciones restringidas o si ya están instaladas, se desactivarán. Al eliminar una aplicación de la lista de aplicaciones restringidas, la aplicación se vuelve a activar si ya está instalada.

BlackBerry UEM incluye un perfil de cumplimiento predeterminado. El perfil de conformidad predeterminado no aplica ninguna condición de conformidad. Para aplicar las reglas de cumplimiento, puede cambiar la configuración del perfil de cumplimiento predeterminado o puede crear y asignar perfiles de cumplimiento personalizados. A las cuentas de usuario que no tengan asignado un perfil de cumplimiento personalizado se les asignará el perfil de cumplimiento predeterminado.

Creación de un perfil de cumplimiento

Antes de empezar:

- Si está definiendo las reglas para restringir o permitir aplicaciones específicas, agregue estas aplicaciones a la lista de aplicaciones restringidas. Para obtener más información, consulte Agregue una aplicación a la lista de aplicaciones restringidas. Tenga en cuenta que esto no se aplica a las aplicaciones integradas para iOS 9.3.2 con supervisión y dispositivos posteriores. Para restringir las aplicaciones integradas, debe crear un perfil de conformidad y agregar las aplicaciones a la lista de aplicaciones restringidas del perfil. Para obtener más información, consulte iOS: configuración del perfil de conformidad.
- Para controlar las aplicaciones en los perfiles de cumplimiento de dispositivos Windows Phone, deberá cargar un AET. Para obtener más información, consulte Carga de un identificador de inscripción de la aplicación para los dispositivos Windows Phone.
- Si desea enviar una notificación de correo electrónico a los usuarios cuando sus dispositivos no cumplan, edite el correo electrónico de cumplimiento predeterminado o cree una nueva plantilla de correo electrónico. Para obtener más información, consulte Cree una plantilla para las notificaciones de conformidad por correo electrónico.

1. En la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Conformidad > Conformidad**.

3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil de cumplimiento.
5. Si desea enviar un mensaje de notificación a los usuarios cuando sus dispositivos no cumplen con los requisitos, realice cualquiera de las acciones siguientes:
   - En la lista desplegable **Mensaje de correo electrónico enviado cuando se detecta infracción**, seleccione una plantilla de correo electrónico. Para ver el correo electrónico de cumplimiento predeterminado, haga clic en Configuración > Configuración general > Plantillas de correo electrónico.
   - En la lista desplegable **Intervalo de cumplimiento**, seleccione la frecuencia con la que BlackBerry UEM comprueba la conformidad.
   - Amplíe **Notificación de dispositivo enviada cuando se detecta una violación de conformidad**. Edite el mensaje si es necesario.

   Si desea utilizar variables para rellenar las notificaciones con información de los usuarios, del dispositivos y del cumplimiento, consulteVariables. También puede definir y utilizar sus propias variables personalizadas mediante la consola de gestión. Para obtener más información, consulteVariables personalizadas.
6. Haga clic en la pestaña para cada tipo de dispositivo en la empresa y configure los valores apropiados para cada configuración de perfil. Para obtener más información acerca de la configuración de cada perfil, consulte Configuración del perfil de conformidad.
7. Haga clic en **Agregar**.

Después de terminar: Si fuera necesario, clasifique los perfiles.

Tareas relacionadas

Asignación de un perfil o una política de TI a un grupo de usuarios
Asignar un perfil o una política de TI a una cuenta de usuario

Cree una plantilla para las notificaciones de conformidad por correo electrónico

Puede crear varias plantillas de correo electrónico, personalizarlas para aplicarlas a determinados tipos de dispositivos o grupos de usuarios y asignar una plantilla apropiada para cada cuenta de usuario. Cuando el dispositivo de un usuario no cumpla con un perfil de conformidad, BlackBerry UEM puede enviar un mensaje de correo electrónico personalizado en función de la plantilla asignada. BlackBerry UEM Incluye una plantilla de correo electrónico predeterminada de infracción de conformidad que se puede editar, pero no borrar. Si no asigna una plantilla diferente a una cuenta de usuario, BlackBerry UEM utiliza la plantilla predeterminada.

1. En la barra de menú, haga clic en **Configuración** > **Configuración general**.
2. Haga clic en **Plantillas de correo electrónico**.
3. Haga clic en +. Seleccione **Infracción de conformidad**.
4. En el campo **Nombre**, escriba un nombre para identificar la plantilla.
5. En el campo **Asunto**, escriba un asunto para el mensaje de correo electrónico.
6. En el campo **Mensaje**, el texto del cuerpo del mensaje de correo electrónico de conformidad. Utilice el editor HTML para seleccionar el formato de fuente y para insertar imágenes, por ejemplo, un logotipo de empresa. Inserte variables en el texto para personalizar el mensaje, por ejemplo, puede utilizar la variable %UserDisplayName% para insertar el nombre del destinatario. Para obtener una lista de variables disponibles, consulte Variables predeterminadas.
7. Haga clic en **Guardar**.

Gestión de perfiles de conformidad de BlackBerry Dynamics

Los perfiles de conformidad de BlackBerry Dynamics se importan desde Good Control cuando sincroniza Good Control con BlackBerry UEM. No puede editar los perfiles de conformidad de BlackBerry Dynamics, pero se pueden utilizar como referencia al crear nuevos perfiles de conformidad en BlackBerry UEM. Los usuarios que se asignaron a un perfil de conformidad en Good Control permanecen asignados al mismo perfil después de que se sincronicen con BlackBerry UEM. Cuando un usuario se asigna a un perfil de conformidad de BlackBerry Dynamics, el perfil de conformidad de BlackBerry Dynamics tiene prioridad sobre las reglas de BlackBerry Dynamics en los perfiles de conformidad de BlackBerry UEM a los que se puede asignar también un usuario.

Para obtener información sobre cómo crear perfiles de conformidad en BlackBerry UEM, consulte Crear un perfil de conformidad.

Configuración	Descripción
SO liberado	Esta configuración especifica las acciones que se producen cuando un usuario o un atacante evita diversas restricciones en un dispositivo para modificar el sistema operativo, instala aplicaciones no aprobadas u obtiene permisos elevados, y las acciones que se producen en las aplicaciones de BlackBerry Dynamics si se utiliza un sistema operativo liberado.
Verificación de la versión del SO	Esta configuración especifica las versiones del SO que están permitidas y restringidas, y las acciones que se producen en las aplicaciones de BlackBerry Dynamics si hay un SO restringido instalado en un dispositivo.
Verificación del modelo del hardware	Esta configuración especifica los modelos de hardware que están permitidos y restringidos, y las acciones que se producen en las aplicaciones de BlackBerry Dynamics si se usa un modelo de hardware restringido.
Verificación de versiones de bibliotecas de BlackBerry Dynamics	Esta configuración especifica las bibliotecas de BlackBerry Dynamics que se pueden usar y las acciones que se producen en las aplicaciones de BlackBerry Dynamics si el dispositivo utiliza una versión no permitida de la biblioteca.
Verificación de la conectividad	Esta configuración especifica si un dispositivo se debe conectar a BlackBerry UEM en un número especificado de días y las acciones que se producen en las aplicaciones de BlackBerry Dynamics si un dispositivo no se conecta a BlackBerry UEM. La configuración secundaria "Basar intervalo de conectividad en las aplicaciones delegadas de la autenticación" especifica si la aplicación configurada como la delegada de la autenticación gestiona el intervalo de conectividad. Si utiliza la aplicación delegada de la autenticación para gestionar el intervalo de conectividad, las aplicaciones que se utilizan con menos frecuencia no se bloquearán ni eliminarán si no se realiza la conexión con ellas. BlackBerry UEM.

Conceptos relacionados

Control de BlackBerry Dynamics en dispositivos de usuarios

Configuración de Enterprise Management Agent

El perfil Enterprise Management Agent se asegura de que los dispositivos se pongan en contacto periódicamente con BlackBerry UEM para actualizar las aplicaciones y la configuración. Cuando hay una actualización para un dispositivo, BlackBerry UEM solicita al dispositivo que se ponga en contacto con BlackBerry UEM para recibir actualizaciones. Si por algún motivo el dispositivo no recibe el aviso, el perfil de Enterprise Management Agent se utiliza para asegurarse de que el dispositivo se pone en contacto con BlackBerry UEM en los intervalos que especifique.

También puede utilizar el perfil Enterprise Management Agent para permitir que BlackBerry UEM pueda recopilar una lista de aplicaciones personales en los dispositivos de los usuarios. Para desactivar la recopilación de aplicaciones personales, debe desmarcar la opción "Permitir recopilaciones de aplicaciones personales". Para obtener más información, consulte Desactivación de la recopilación de aplicaciones personales.

Para dispositivos con BlackBerry 10, el perfil de Enterprise Management Agent permite restringir los paquetes de cifrado de la biblioteca SSL compatibles con el dispositivo. La restricción de los paquetes de cifrado compatibles no afecta a la comunicación del dispositivo con BlackBerry UEM, pero podría afectar a la comunicación con otros servidores de la empresa, en función de los requisitos de dichos servidores.

Se puede asignar un perfil de Enterprise Management Agent a usuarios, a grupos de usuarios y a grupos de dispositivos.

Creación de un perfil de Enterprise Management Agent

1. En la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Política > Enterprise Management Agent**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil.
5. Establezca los valores para cada tipo de dispositivo que requiera la empresa. Para obtener más información acerca de la configuración del perfil, consulte Ajustes del perfil de Enterprise Management Agent.
6. Haga clic en **Agregar**.

Después de terminar: Si fuera necesario, clasifique los perfiles.

Conceptos relacionados

Ajustes del perfil de Enterprise Management Agent

Tareas relacionadas

Asignación de un perfil o una política de TI a un grupo de usuarios
Asignar un perfil o una política de TI a una cuenta de usuario

Limitación de los dispositivos a una única aplicación

En los dispositivos iOS supervisados, los dispositivos Android gestionados mediante Samsung KNOX MDM o los dispositivos Windows 10 Enterprise y Windows 10 Education gestionados mediante MDM, puede usar un perfil de modo de bloqueo de aplicaciones para limitar los dispositivos y que solo se ejecute una aplicación. Por ejemplo, puede limitar el acceso a una sola aplicación con fines de formación o bien para realizar demostraciones

en el punto de venta. En los dispositivos iOS, el botón de inicio está desactivado y en el dispositivo se abre automáticamente la aplicación cuando el usuario activa el dispositivo o lo reinicia.

Crear un perfil de modo de bloqueo de la aplicación

Especifique una única aplicación para que se ejecute en los dispositivos y seleccione los ajustes del dispositivo que desea activar para el usuario. Para los dispositivos iOS supervisados, puede seleccionar una aplicación en la lista de aplicaciones, especificar el ID de paquete de la aplicación o seleccionar una aplicación integrada. Para los dispositivos Android que se administran mediante Samsung KNOX MDM, especifique el identificador de paquete de la aplicación que desea establecer como pantalla de inicio. Para los dispositivos Windows 10 gestionados con MDM, especifique la cuenta y el ID de modelo de usuario de la aplicación (AUMID) de la aplicación. Visite docs.microsoft.com para buscar el AUMID.

Nota: Si el usuario no instala la aplicación en un dispositivo, cuando asigne el perfil a un usuario o a un grupo de usuarios el dispositivo no se limitará a la aplicación.

Antes de empezar: Para los dispositivos iOS, si tiene pensado utilizar la lista de aplicaciones para seleccionar una aplicación, asegúrese de que la aplicación esté disponible en la lista de aplicaciones.

1. En la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Política > Modo de bloqueo de la aplicación**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil.
5. Especifique los tipos de dispositivos a los que se aplica el perfil.
6. Lleve a cabo una de las tareas siguientes:

Tarea	Pasos
Especificar la aplicación que se va a ejecutar en los dispositivos iOS	En la sección **Especificar la aplicación que se va a ejecutar en el dispositivo**, realice una de las siguientes acciones: • Haga clic en **Agregar una app** y haga clic en una aplicación de la lista. • Haga clic en **Especificar el ID de paquete de una aplicación** y escriba el ID de paquete (por ejemplo, <*com.company.appname*>). Los caracteres válidos son letras mayúsculas y minúsculas, números del 0 al 9, el guion (-) y el punto (.). • Haga clic en **Seleccionar una aplicación de iOS integrada** y seleccione una aplicación de la lista desplegable.
Especificar la aplicación que se va a ejecutar en los dispositivos Android	En el campo **Especificar la aplicación que se va a ejecutar en el dispositivo**, escriba el identificador de paquete de la aplicación que desea establecer como pantalla de inicio. Por ejemplo, si quiere que BBM Meetings sea la aplicación, escriba `com.blackberry.bbm.meetings`.

Tarea	Pasos
Especificar la aplicación que se va a ejecutar en los dispositivos Windows 10	• En el campo **Cuenta**, escriba el nombre de la cuenta de usuario que incluya el nombre de dominio y el nombre de usuario. Para un usuario local, utilice el nombre del dispositivo en lugar del nombre de dominio. • En el campo **ID de modelo de usuario de la aplicación**, escriba el AUMID de la aplicación (por ejemplo, el AUMID de la aplicación Calculadora es `Microsoft.WindowsCalculator_8wekyb3d8bbwe!App`.

7. Para los dispositivos iOS y Android, en **Configuración para el administrador**, seleccione las opciones que desee activar para el usuario al utilizar la aplicación.
8. Para los dispositivos iOS, en **Configuración para el usuario**, seleccione las opciones que el usuario puede activar.
9. Haga clic en **Agregar**.

Después de terminar: Si fuera necesario, clasifique los perfiles.

Tareas relacionadas

Adición de una aplicación de Android a la lista de aplicaciones si BlackBerry UEM no está configurado para dispositivos Android Enterprise
Adición de una aplicación de Android a la lista de aplicaciones si BlackBerry UEM está configurado para Android Enterprise
Adición de una aplicación de iOS a la lista de aplicaciones
Asignación de un perfil o una política de TI a un grupo de usuarios
Asignar un perfil o una política de TI a una cuenta de usuario

Control de las versiones de software instaladas en los dispositivos

Puede controlar las versiones de software del dispositivo instaladas en dispositivos Android con activaciones Solo espacio de trabajo, dispositivos con Samsung KNOX y dispositivos con BlackBerry 10.

En dispositivos con Android 6.0 y posteriores activados con Solo espacio de trabajo, puede especificar si el usuario pude elegir cuándo instalar las actualizaciones de software disponibles o si estas se instalan automáticamente. Puede especificar reglas diferentes en función del modelo de dispositivo y la versión del sistema operativo instalada actualmente.

En dispositivos con Samsung KNOX, puede utilizar Enterprise Firmware Over the Air (E-FOTA) para controlar cuándo se instalan las actualizaciones de firmware de Samsung. El control de las versiones garantiza que los dispositivos de los usuarios utilizan las versiones de firmware compatibles con sus aplicaciones y cumplen las políticas de su empresa. Puede utilizar un perfil de Requisitos de solicitud de servicio del dispositivo para crear reglas de firmware para los dispositivos Samsung KNOX activados en UEM. Puede programar cuándo se instalan las actualizaciones de firmware y especificar cuándo se deben instalar actualizaciones forzosas. Para obtener más información sobre E-FOTA, visite https://seap.samsung.com/sdk/enterprise-fota.

En los dispositivos que ejecutan BlackBerry 10 OS versión 10.3.1 o posteriores activados con Trabajo y personal - Regulado o con Solo espacio de trabajo, puede limitar las versiones de software que los dispositivos con BlackBerry 10 pueden tener instaladas mediante un perfil de Requisitos de solicitud de servicio del dispositivo. También puede agregar excepciones en la configuración general para modelos de dispositivos

específicos. Por ejemplo, puede que desee probar una versión de software antes de ponerlo a disposición de la empresa.

Para aplicar una acción determinada si la versión de software restringida se instala en un dispositivo, debe crear un perfil de cumplimiento y asignarlo a los usuarios, los grupos de usuarios o los grupos de dispositivos. El perfil de cumplimiento especifica las acciones que se llevan a cabo si el usuario no elimina la versión de software restringida del dispositivo.

Crear un perfil de requisitos de solicitud de servicio del dispositivo para dispositivos Android con activaciones Solo espacio de trabajo

Antes de empezar: Compruebe que se ha agregado una licencia de E-FOTA a BlackBerry UEM. Para agregar una licencia, consulte Añadir una licencia de E-FOTA en el contenido de Configuración.

1. En la barra de menú, haga clic en **Políticas y perfiles**.
2. Haga clic en **Conformidad > Requisitos de solicitud de servicio del dispositivo**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil.
5. Haga clic en la pestaña **Android**.
6. En la tabla **Regla de actualización del SO Solo espacio de trabajo**, haga clic en +.
7. En la lista desplegable **Modelo de dispositivo**, seleccione un modelo de dispositivo.
8. En la lista desplegable **Versión del SO**, seleccione la versión del sistema operativo.
9. En la lista **Regla de actualización**, seleccione una de las opciones siguientes.
   - Seleccione **Predeterminado** para permitir que el usuario elija cuánto instalar las actualizaciones.
   - Seleccione **Actualizar automáticamente** para instalar las actualizaciones sin preguntar al usuario.
   - Seleccione **Actualizar automáticamente entre** para instalar las actualizaciones entre las horas especificadas sin preguntar al usuario. El usuario puede elegir que las actualizaciones se instalen fuera de este intervalo.
   - Seleccione **Retrasar hasta 30 días** para bloquear la instalación de actualizaciones durante 30 días. Después de 30 días, el usuario puede elegir cuándo se instalan las actualizaciones. En del fabricante del dispositivo y el proveedor de servicios inalámbricos, puede que las actualizaciones de seguridad no se retrasen.
10. Cuando haya terminado, haga clic en **Agregar**.
11. Repita los pasos del 6 al 10 para cada regla que desee agregar.
12. Haga clic en **Agregar**.

Después de terminar: Si fuera necesario, clasifique los perfiles.

Crear un perfil de requisitos de solicitud de servicio del dispositivo para dispositivos con Samsung KNOX

1. En la barra de menú, haga clic en **Políticas y perfiles**.
2. Haga clic en **Conformidad > Requisitos de solicitud de servicio del dispositivo**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil.
5. Haga clic en la pestaña **Android**.
6. En la tabla **Reglas de firmware del dispositivo Samsung**, haga clic en +.

7. En el campo **Modelo de dispositivo**, introduzca el modelo de dispositivo o seleccione uno en la lista desplegable.
8. En la lista desplegable **Idioma**, seleccione un idioma.
9. En el campo **Código del operador**, introduzca el código CSC del proveedor de servicios inalámbricos para el dispositivo.
10. Haga clic en **Obtener versión de firmware**.
11. Repita los pasos del 5 al 8 para cada regla de firmware que desee agregar.
12. Cuando haya terminado, haga clic en **Agregar**.
13. En la tabla **Reglas de firmware del dispositivo Samsung**, haga clic en **Horario** junto a la versión de firmware que ha agregado.
14. En el cuadro de diálogo **Programar actualización forzada**, haga lo siguiente:
    a) En los campos **Programar actualización forzada entre**, seleccione el intervalo de fechas en el que se debe instalar la actualización. El intervalo de fechas debe estar entre 3 y 7 días. El valor predeterminado es 7 días.
    b) En las listas desplegables **Programar actualización forzada durante las horas de**, especifique cuándo se debe instalar la actualización forzada y la zona horaria del usuario. El intervalo de tiempo debe estar entre 1 y 12 horas.
15. Haga clic en **Guardar**.

Después de terminar: Si fuera necesario, clasifique los perfiles.

Crear un perfil de requisitos de solicitud de servicio del dispositivo para dispositivos con BlackBerry 10

Antes de empezar: Cree o edite un perfil de cumplimiento que especifique las acciones que se producen si se instala una versión restringida de software en un dispositivo.

1. En la barra de menú, haga clic en **Políticas y perfiles**.
2. Haga clic en **Conformidad > Requisitos de solicitud de servicio del dispositivo**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil.
5. Haga clic en la pestaña **BlackBerry**.
6. Para ver una lista de todas las versiones de software del dispositivo y del proveedor de servicios correspondiente, del modelo de dispositivo, del ID de hardware, de la versión de software y de la información del estado de revocación para el dispositivo con BlackBerry 10, haga clic en **Ver una lista de versiones de software para el dispositivo**.
7. Seleccione la casilla de verificación **Hacer actualización obligatoria** para obligar a los usuarios a actualizar sus dispositivos con una versión de software definida en el perfil.
8. En el campo **Periodo de gracia**, escriba un valor, en horas, que puede transcurrir antes de que los usuarios deban actualizar sus dispositivos. Si los usuarios no actualizan sus dispositivos dentro del periodo de gracia, o si establece el periodo de gracia a 0, la actualización del software se instala automáticamente en los dispositivos.
9. En la lista desplegable **Versión mínima de software**, seleccione la versión mínima de software que un dispositivo con BlackBerry 10 debe estar ejecutando.
10. En la lista desplegable **Versión máxima de software**, seleccione la versión máxima de software que un dispositivo con BlackBerry 10 debe estar ejecutando.
11. Para anular la configuración global para un modelo de dispositivo, realice las tareas siguientes:
    a) En la tabla **Excepciones**, haga clic en +.
    b) En la lista desplegable **Disposición**, seleccione si desea permitir o no permitir las versiones de software. Si especifica un rango no permitido, y no ha especificado un rango permitido para un modelo de dispositivo,

aparecerá una segunda columna en donde se le pedirá que especifique un rango permitido. Si un rango permitido no se especifica, la configuración general ya no se aplicará al modelo de dispositivo y todas las versiones de software que no sean la excepción estarán permitidas automáticamente.

c) En la lista desplegable **Modelo de dispositivo**, seleccione el modelo de dispositivo al que quiera asignar la excepción.
d) En la lista desplegable **Mínima**, seleccione la versión mínima de software que desee permitir o no permitir.
e) En la lista desplegable **Máxima**, seleccione la versión máxima de software que desee permitir o no permitir.
f) Si rechaza una versión de software, seleccione la versión mínima de software que desee permitir.
g) Si rechaza una versión de software, seleccione la versión máxima de software que desee permitir.

12. Haga clic en **Guardar**.

13. Haga clic en **Agregar**.

Después de terminar: Si fuera necesario, clasifique los perfiles.

Tareas relacionadas

Asignación de un perfil o una política de TI a un grupo de usuarios
Asignar un perfil o una política de TI a una cuenta de usuario

Presentación de los usuarios que están ejecutando una versión de software rechazada

Puede ver una lista de los usuarios que están ejecutando una versión de software rechazada. Una versión de software rechazada es una versión de software que un proveedor de servicios ya no acepta, pero que aún se puede instalar en el dispositivo del usuario.

1. En la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Conformidad > Requisitos de solicitud de servicio del dispositivo**.
3. Haga clic en el nombre del perfil que desea consultar.
4. Haga clic en la pestaña **x usuarios con versión de informe especial rechazada** para ver la lista de usuarios que están ejecutando una versión de software rechazada.

Presentación de la información de la empresa en los dispositivos

Puede configurar BlackBerry UEM para mostrar la información de la empresa y avisos de empresa personalizados en los dispositivos.

Para los dispositivos con BlackBerry 10, iOS, macOS, Android y Windows 10, puede crear avisos de empresa personalizados para que se muestren durante la activación. Por ejemplo, un aviso puede contener las condiciones que un usuario debe seguir para cumplir con los requisitos de seguridad de la empresa. El usuario debe aceptar el aviso para continuar con el proceso de activación. Puede crear varios avisos para cubrir diferentes requisitos y puede crear versiones separadas de cada aviso para que sean compatibles con idiomas diferentes.

Puede crear perfiles de dispositivo para mostrar información sobre la empresa en los dispositivos. En los dispositivos iOS, Android y Windows Phone, la información de la empresa se muestra en BlackBerry UEM Client en el dispositivo. En Windows 10, el número de teléfono y la dirección de correo se muestran en la información de soporte en el dispositivo. En los dispositivos con BlackBerry 10 y Samsung KNOX, puede utilizar el perfil de dispositivo para mostrar el aviso de empresa personalizado cuando el usuario reinicia el dispositivo.

En los dispositivos con BlackBerry 10, Samsung KNOX y iOS supervisados, también puede utilizar el perfil de dispositivo para añadir una imagen de fondo de pantalla personalizada con la información que se debe mostrar a los usuarios. Por ejemplo, puede crear una imagen que contenga la información de asistencia y

contacto, la información interna de la página web o el logotipo de la empresa. En los dispositivos con BlackBerry 10 y Samsung KNOX, el fondo de pantalla se muestra en el espacio de trabajo.

Dónde se muestra la información de la empresa	Cómo configurar la información de la empresa
Mostrar un aviso de la empresa al realizar la activación en los dispositivos con BlackBerry 10, iOS, macOS, Android y Windows 10	Cree un aviso de la empresa y asígnelo a un perfil de activación.
Mostrar un aviso de la empresa al reiniciar en los dispositivos Samsung KNOX	Cree un aviso de la empresa y asígnelo en la pestaña Android del perfil de dispositivo. Para cambiar el aviso que aparece al reiniciar el dispositivo, debe actualizar el perfil de dispositivo.
Mostrar un aviso de la empresa al reiniciar en los dispositivos BlackBerry 10	Cree un aviso de la empresa y asígnelo en la pestaña BlackBerry del perfil de un dispositivo. Compruebe que se ha seleccionado la regla de política de TI "Mostrar aviso de la organización después de reiniciar el dispositivo". Para cambiar el aviso que aparece al reiniciar el dispositivo, debe actualizar el perfil de dispositivo. **Nota:** La regla de política de TI se aplica solo a los tipos de activación "Solo espacio de trabajo" y "Trabajo y personal: regulado" en los dispositivos que ejecutan BlackBerry 10 OS versión 10.3.1 y posteriores.
Mostrar la información de la empresa en BlackBerry UEM Client en los dispositivos iOS, Android o Windows Phone, o en la información de soporte técnico en los dispositivos Windows 10.	Escriba la información que quiere que se muestre en la pestaña correspondiente del perfiles de dispositivo.
En una imagen de fondo de pantalla en los dispositivos con BlackBerry 10, Samsung KNOX o iOS supervisados	Seleccione un archivo de imagen en la pestaña correspondiente del perfiles de dispositivo.

Crear avisos de la empresa

Puede crear avisos de empresa personalizados para que se muestren durante la activación de los dispositivos con BlackBerry 10, iOS, macOS, Android y Windows 10.

Los dispositivos con BlackBerry 10 y Samsung KNOX también pueden mostrar el aviso de la empresa cuando un usuario los reinicia.

1. En la barra de menús, haga clic en **Configuración**.
2. En el panel izquierdo, amplíe **Configuración general**.
3. Haga clic en **Avisos de la organización**.
4. Haga clic en + en el lateral derecho de la pantalla.
5. En el campo **Nombre**, escriba un nombre para el aviso de la empresa.
6. Opcionalmente, puede reutilizar el texto de otro aviso de la empresa seleccionándolo en la lista desplegable **Texto copiado del aviso de la organización**.

7. En la lista desplegable **Idioma del dispositivo**, seleccione el idioma que desea utilizar como el idioma predeterminado para el aviso de la empresa.
8. En el campo **Aviso de la organización**, escriba el texto del aviso de la empresa.
9. Opcionalmente, puede hacer clic varias veces en **Agregar un idioma adicional** para publicar el aviso de la empresa en más idiomas.
10. Si publica el aviso de la empresa en más de un idioma, seleccione la opción **Idioma predeterminado** debajo de uno de los mensajes para convertirlo en el idioma predeterminado.
11. Haga clic en **Guardar**.

Después de terminar:

- Para mostrar el aviso de la empresa durante la activación, asigne el aviso de la empresa a un perfil de activación.
- Para mostrar el aviso de la empresa cuando se reinicie un dispositivo con Samsung KNOX, asigne el aviso de la empresa a un perfil de dispositivo.
- Para mostrar el aviso de la empresa cuando un dispositivo con BlackBerry 10 se reinicia, asigne el aviso de la empresa a un perfil del dispositivo y seleccione la regla de política de TI "Mostrar aviso de la organización después de reiniciar el dispositivo".

Creación de un perfil de dispositivo

Antes de empezar: En los dispositivos BlackBerry 10 y Samsung KNOX, cree avisos de la empresa.

1. En la barra de menú, haga clic en **Policies and Profiles (Políticas y perfiles)**.
2. Haga clic en **Personalizada > Dispositivo**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil. Cada perfil de dispositivo debe tener un nombre único.
5. Lleve a cabo una de las tareas siguientes:

Tarea	Pasos
Asignación de un aviso de la empresa para que se muestre en los dispositivos BlackBerry 10 o Samsung KNOX mientras se reinician	a. Haga clic en **BlackBerry** o **Android**. b. En la lista desplegable **Asignar aviso de la organización**, seleccione el aviso de la empresa que desea que se muestre en los dispositivos.
En iOS, Android o Windows Phone, defina la información de la empresa que se mostrará en la aplicación BlackBerry UEM Client. En Windows 10, defina el número de teléfono y la dirección de correo que se mostrarán en la información de soporte en los dispositivos.	a. Haga clic en **iOS**, **Android** o **Windows**. b. Escriba el nombre, dirección, número de teléfono y dirección de correo de la empresa.

6. Si fuera necesario, realice las tareas siguientes:

Tarea	Pasos
Adición de una imagen de fondo de pantalla al espacio de trabajo de los dispositivos BlackBerry 10 o Samsung KNOX	**a.** Haga clic en **BlackBerry** o **Android**. **b.** En la sección **Fondo de pantalla del espacio de trabajo**, haga clic en **Examinar**. **c.** Seleccione la imagen que desea utilizar como fondo de pantalla. **d.** Haga clic en **Abrir**.
Añadir una imagen de fondo de pantalla a los dispositivos iOS supervisados	**a.** Haga clic en **iOS**. **b.** En la sección **Fondo de pantalla del dispositivo**, seleccione si el fondo de pantalla debe mostrarse en la **Pantalla de inicio**, la **Pantalla de bloqueo** o **Ambas**. **c.** Haga clic en **Examinar** y seleccione la imagen que desea utilizar como fondo de pantalla. **d.** Haga clic en **Abrir**. **e.** En el campo **Configurar el fondo de pantalla para**, seleccione el lugar donde desea que se muestre el fondo de pantalla.

7. Haga clic en **Add (Agregar)**.

Después de terminar:

- Para mostrar el aviso de la empresa cuando un dispositivo con BlackBerry 10 se reinicia, seleccione la regla de política de TI "Mostrar aviso de la empresa después de reiniciar el dispositivo".
- Si fuera necesario, clasifique los perfiles.

Tareas relacionadas

Asignación de un perfil o una política de TI a un grupo de usuarios
Asignar un perfil o una política de TI a una cuenta de usuario

Uso de servicios de ubicación en los dispositivos

Puede utilizar un perfil de servicio de ubicación para solicitar la ubicación de los dispositivos y ver las ubicaciones aproximadas en un mapa. También puede autorizar a los usuarios a localizar sus dispositivos mediante BlackBerry UEM Self-Service. Si activa el historial de ubicaciones para los dispositivos iOS y Android, los dispositivos deben aportar información sobre la ubicación de forma periódica y los administradores pueden ver el historial de ubicaciones.

Los perfiles de los servicios de ubicación utilizan los servicios de ubicación en los dispositivos iOS, Android y Windows 10 Mobile. En función del dispositivo y de los servicios disponibles, es posible que los servicios de ubicación utilicen información móvil, de GPS y redes Wi-Fi para determinar la ubicación del dispositivo.

Configurar las opciones del servicio de ubicación

Puede configurar las opciones de los perfiles de servicio de ubicación, como la unidad de velocidad que se muestra en un dispositivo al ver su ubicación en un mapa. Si habilita el historial de ubicaciones en los dispositivos iOS y Android, BlackBerry UEM almacena el historial de ubicaciones durante un mes de manera predeterminada.

1. En la barra de menú, haga clic en **Configuración > Configuración general > Servicio de ubicación**.

2. En el campo **Antigüedad del historial de ubicación**, especifique el número de días, semanas o meses que BlackBerry UEM debe guardar el historial de ubicaciones de los dispositivos.
3. En la lista desplegable **Unidad de velocidad mostrada** haga clic en **km/h** o **mph**.
4. Haga clic en **Guardar**.

Creación de un perfil de servicio de ubicación

Puede asignar un perfil del servicio de ubicación a cuentas de usuario, grupos de usuarios o grupos de dispositivos. Los usuarios deben aceptar el perfil con anterioridad para que la consola de gestión o BlackBerry UEM Self-Service muestren las ubicaciones de los dispositivos iOS y Android en un mapa.Los dispositivos Windows 10 Mobile aceptan automáticamente el perfil.

Antes de empezar: Configurar las opciones del servicio de ubicación

1. En la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Protección > Servicio de ubicación**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil de servicio de ubicación.
5. Opcionalmente, desactive la casilla de verificación para cualquier tipo de dispositivo para el que no desee configurar el perfil.
6. Lleve a cabo cualquiera de las tareas siguientes:

Tarea	Pasos
Activar el historial de ubicaciones en dispositivos iOS	**a.** En la pestaña **iOS**, compruebe que la casilla de verificación **Registrar historial de ubicaciones de dispositivo** está seleccionada. **Nota:** BlackBerry UEM recopila la ubicación de un dispositivo cada hora y, si es posible, cuando haya un cambio significativo en la ubicación del dispositivo (por ejemplo, 500 metros o más).
Activar el historial de ubicaciones en dispositivos Android	**a.** En la pestaña **Android**, compruebe que la casilla de verificación **Registrar historial de ubicaciones de dispositivo** está seleccionada. **b.** En el campo **Distancia de comprobación de ubicación de dispositivo**, especifique la distancia mínima que un dispositivo debe recorrer antes de que se actualice la ubicación del dispositivo. **c.** En el campo **Frecuencia de actualización de la ubicación**, especifique con qué frecuencia se actualiza la ubicación del dispositivo. **Nota:** Se deben cumplir las condiciones de distancia y frecuencia antes de que se actualice la ubicación del dispositivo.

7. Haga clic en **Add (Agregar)**.

Después de terminar: Si fuera necesario, clasifique los perfiles.

Tareas relacionadas

Asignación de un perfil o una política de TI a un grupo de usuarios
Asignar un perfil o una política de TI a una cuenta de usuario

Desactivación de las notificaciones fuera de las horas laborables

Puede utilizar perfiles de no molestar para bloquear las notificaciones de dispositivos fuera de las horas laborables en BlackBerry Work for Android y BlackBerry Work for iOS. Esta función requiere BEMS 2,8 o posterior.

Crear un perfil de no molestar

Antes de empezar:

- BEMS 2.8 o posterior está instalado y configurado en su entorno. Para obtener instrucciones, consulte las BEMS guías de instalación y configuración.
- BlackBerry Work se agrega al perfil de conectividad de BlackBerry Dynamics. Consulte Configurar los ajustes de conexión de BlackBerry Work en el BlackBerry Work contenido de administración.

1. En la barra de menú, haga clic en **Políticas y perfiles**.
2. Haga clic en **Protección > No molestar**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil.
5. Introduzca un mensaje para que se muestre en los dispositivos cuando las notificaciones de BlackBerry Work están bloqueadas. Si deja este campo en blanco, se mostrará un mensaje predeterminado.
6. Lleve a cabo una de estas acciones:

Tarea	Pasos
Especifique días y horas de trabajo comunes.	**a.** Haga clic en la opción **Seleccionar días y horas de trabajo comunes**. **b.** En las listas desplegables **De**, especifique la hora de inicio de los días de trabajo. **c.** En las listas desplegables **Para**, especifique la hora de finalización de los días de trabajo. **d.** En la lista **Días de trabajo**, seleccione los días de la semana que son días de trabajo.
Especifique horas de trabajo personalizadas para días específicos.	**a.** Haga clic en la opción **Seleccionar días y horas de trabajo personalizadas**. **b.** Seleccione un día de la semana. **c.** En las listas desplegables **De**, especifique la hora de inicio del día de trabajo. **d.** En las listas desplegables **Para**, especifique la hora de finalización del día de trabajo. **e.** Repita los pasos del 2 al 4 para cada día de la semana que sea un día de trabajo.

7. Haga clic en **Agregar**.

Administración de las características de iOS mediante perfiles de carga personalizados

Se pueden utilizar perfiles de carga personalizados para controlar las funciones de dispositivos iOS que no están controladas por las políticas o perfiles de BlackBerry UEM.

Nota: Si una característica está controlada por una política o perfil de BlackBerry UEM, un perfil de carga personalizado puede que no funcione como se espera. Debería utilizar las políticas o perfiles actuales, siempre que sea posible.

Puede crear perfiles de configuración de Apple mediante Apple Configurator y agregarlos a perfiles de carga personalizados de BlackBerry UEM. Se pueden asignar perfiles de carga personalizados a usuarios, grupos de usuarios y grupos de dispositivos.

- Controle una característica de iOS que no esté incluida en las políticas y los perfiles de BlackBerry UEM. Por ejemplo, con BES10, el asistente de CEO fue capaz de acceder tanto a su propia cuenta de correo como a la del CEO en un iPhone. En BlackBerry UEM, solo se puede asignar un perfil de correo a un dispositivo, de modo que el asistente solo puede tener acceso a su propia cuenta. Para resolver este problema, puede asignar un perfil de correo que permita al iPhone del asistente acceder a la cuenta de correo de este y a un perfil de carga personalizado que permita al iPhone de asistente acceder a la cuenta de correo del CEO.
- Controle una nueva característica de iOS que se lanzó después de la última versión de software de BlackBerry UEM. Por ejemplo, desea controlar una nueva característica que estará disponible para los dispositivos cuando actualicen a iOS 9, pero BlackBerry UEM no tendrá un perfil para la nueva característica hasta la próxima versión de software de BlackBerry UEM. Para resolver este problema, puede crear un perfil de carga personalizado que controle esa función hasta la próxima versión de software de BlackBerry UEM.

Creación de un perfil de carga personalizado

Antes de empezar: Descargue e instale la última versión de Apple Configurator de Apple.

1. En Apple Configurator, cree un perfil de configuración de Apple.
2. En la consola de gestión de BlackBerry UEM, haga clic en **Políticas y perfiles**.
3. Haga clic en **Personalizada > Cargas personalizadas**.
4. Haga clic en +.
5. Escriba un nombre y una descripción para el perfil.
6. En Apple Configurator, copie el código XML para el perfil de configuración de Apple. Cuando copie el texto, copie únicamente los elementos en negrita como se muestra en el ejemplo de código siguiente.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/
DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
     <key>PayloadContent</key>
     <array>
          <dict>
               <key>CalDAVAccountDescription</key>
               <string>CalDAV Account Description</string>
               <key>CalDAVHostName</key>
               <string>caldav.server.example</string>
               <key>CalDAVPort</key>
               <integer>8443</integer>
               <key>CalDAVPrincipalURL</key>
               <string>Principal URL for the CalDAV account</string>
```

```
                <key>CalDAVUseSSL</key>
                </true>
                <key>CalDAVUsername</key>
                <string>Username</string>
                <key>PayloadDescription</key>
                <string>Configures CalDAV account.</string>
                <key>PayloadDisplayName</key>
                <string>CalDAV (CalDAV Account Description)</string>
                <key>PayloadIdentifier</key>
                <string>.caldav1</string>
                <key>PayloadOrganization</key>
                <string></string>
                <key>PayloadType</key>
                <string>com.apple.caldav.account</string>
                <key>PayloadUUID</key>
                <string>9ADCF5D6-397C-4E14-848D-FA04643610A3</string>
                <key>PayloadVersion</key>
                <integer>1</integer>
            </dict>
    </array>
    <key>PayloadDescription</key>
    <string>Profile description.</string>
    <key>PayloadDisplayName</key>
    <string>Profile Name</string>
    <key>PayloadOrganization</key>
    <string></string>
    <key>PayloadRemovalDisallowed</key>
    <false/>
    <key>PayloadType</key>
    <string>Configuration</string>
    <key>PayloadUUID</key>
    <string>7A5F8391-5A98-46EA-A3CF-C0D6EDC74632</string>
    <key>PayloadVersion</key>
    <integer>1</integer>
</dict>
</plist>
```

7. En el campo **Carga personalizada**, pegue el código XML de Apple Configurator.
8. Haga clic en **Agregar**.

Tareas relacionadas

Asignación de un perfil o una política de TI a un grupo de usuarios
Asignar un perfil o una política de TI a una cuenta de usuario

Configurar el diseño de las aplicaciones en dispositivos iOS supervisados

Puede controlar el orden de las aplicaciones que se muestran en el dispositivo iOS de un usuario. Este perfil se puede utilizar únicamente con dispositivos con iOS 9.3 y versiones posteriores supervisados.

1. En la barra de menú, haga clic en **Políticas y perfiles**.
2. Haga clic en **Personalizada > Diseño de la pantalla de inicio**.
3. Haga clic en +.

4. En la lista **Tipo de aplicación**, seleccione el tipo de aplicación que desea arrastrar y soltar en la pantalla (por ejemplo, Aplicaciones incorporadas).
5. Arrastre y suelte los iconos de la lista de aplicaciones a la pantalla de inicio.
6. Haga clic en **Agregar**.

Configuración de Windows Information Protection para dispositivos con Windows 10

Puede configurar Windows Information Protection (WIP) para dispositivos con Windows 10 cuando desee:

- Separar los datos personales y del trabajo en los dispositivos y poder borrar solo los datos de trabajo
- Evitar que los usuarios compartan los datos de trabajo fuera de aplicaciones de trabajo protegidas o con personas que no forman parte de su empresa
- Proteger los datos incluso si se mueven o se comparten en otros dispositivos, como una memoria USB
- Auditar el comportamiento de los usuarios y realizar las acciones correspondientes para evitar pérdidas de datos

Al configurar WIP para los dispositivos, puede especificar las aplicaciones que desea proteger con WIP. Las aplicaciones protegidas son de confianza para crear y acceder a los archivos de trabajo, mientras que a las aplicaciones sin protección se les puede bloquear el acceso a los archivos de trabajo. Puede elegir el nivel de protección para aplicaciones protegidas en función de cómo desea que los usuarios se comporten al compartir los datos de trabajo. Cuando está activada la WIP, todas las prácticas de intercambio se auditan. Para obtener más información sobre WIP, visite https://technet.microsoft.com/itpro/windows/keep-secure/protect-enterprise-data-using-wip.

Las aplicaciones que especifique pueden habilitarse o inhabilitarse para la empresa. Las aplicaciones habilitadas pueden crear y acceder a los datos personales y de trabajo. Las aplicaciones inhabilitadas solo pueden crear y acceder a los datos del trabajo. Para obtener más información sobre las aplicaciones habilitadas e inhabilitadas, visite https://technet.microsoft.com/itpro/windows/keep-secure/enlightened-microsoft-apps-and-wip.

Creación de un perfil de Windows Information Protection

1. En la barra de menú, haga clic en **Policies and Profiles (Políticas y perfiles)**.
2. Haga clic en **Protección > Windows Information Protection**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil.
5. Configure los valores adecuados para la configuración de cada perfil. Para obtener más información acerca de la configuración de cada perfil, consulte Windows 10: configuración de perfil de Windows Information Protection.
6. Haga clic en **Agregar**.

Conceptos relacionados

Configuración del perfil de Windows Information Protection

Tareas relacionadas

Asignación de un perfil o una política de TI a un grupo de usuarios
Asignar un perfil o una política de TI a una cuenta de usuario

Aplicaciones

Puede crear una biblioteca de aplicaciones que desee administrar y supervisar en los dispositivos con BlackBerry 10, iOS, Android y Windows. Para administrar aplicaciones, puede agregar las aplicaciones a la lista de aplicaciones y asignarlas a cuentas de usuario, a grupos de usuarios o a grupos de dispositivos.

Al administrar aplicaciones, realice las acciones siguientes:

Paso	Acción
1	Agregue las aplicaciones públicas e internas que desea administrar a la lista de aplicaciones.
2	Cree grupos de aplicaciones para administrar varias aplicaciones al mismo tiempo.
3	Asigne aplicaciones o grupos de aplicaciones a las cuentas de usuario, a los grupos de usuarios o a los grupos de dispositivos para que los usuarios puedan instalarlos.

Adición de aplicaciones a la lista de aplicaciones

La lista de aplicaciones contiene las aplicaciones que se pueden asignar a los usuarios, a los grupos de usuarios y a los grupos de dispositivos. Las aplicaciones que aparecen con un icono de candado son aplicaciones de BlackBerry Dynamics.

Nota: Si su empresa usa Microsoft Intune para MAM de aplicaciones como Office 365, en lugar de agregar las aplicaciones a la lista de aplicaciones, cree un perfil de protección de aplicación de Microsoft Intune para asignar las aplicaciones protegidas por Intunea los usuarios.

Adición de aplicaciones públicas a la lista de aplicaciones

Una aplicación pública es una aplicación que está disponible en la tienda de BlackBerry World, la tienda en línea App Store, la tienda Google Play o Windows Store.

Adición de una aplicación BlackBerry a la lista de aplicaciones

1. En la barra de menú, haga clic en **Aplicaciones**.
2. Haga clic en .
3. Haga clic en **BlackBerry World**.
4. En el campo de búsqueda, busque la aplicación que desea agregar. Puede buscar por el nombre de la aplicación, el proveedor o la URL de BlackBerry World.
5. En la lista desplegable, seleccione el país de la tienda en la que desea buscar.
6. Haga clic en **Buscar**.
7. En los resultados de búsqueda, haga clic en **Agregar** para agregar una aplicación.
8. Para filtrar las aplicaciones BlackBerry en la lista de aplicaciones por categoría, puede seleccionar una categoría para la aplicación. En la lista desplegable **Categoría**, realice una de las acciones siguientes:

Opción	
Seleccione una categoría para la aplicación	**a.** En la lista desplegable, seleccione una categoría.
Cree una categoría para la aplicación	**a.** Escriba un nombre para la categoría. La nueva categoría aparecerá en la lista desplegable con la etiqueta "nueva categoría" a su lado **b.** Pulse **Intro**. **c.** Pulse **Intro**.

9. En la pantalla de información de la aplicación, haga clic en **Agregar**.

Tareas relacionadas

Asignación de una aplicación a un grupo de usuarios
Asignación de una aplicación a una cuenta de usuario

Adición de una aplicación de iOS a la lista de aplicaciones

1. En la barra de menú, haga clic en **Aplicaciones**.
2. Haga clic en .
3. Haga clic en **Tienda de aplicaciones**.
4. En el campo de búsqueda, busque la aplicación que desea agregar. Puede buscar por el nombre de la aplicación, el proveedor o la URL de App Store.
5. En la lista desplegable, seleccione el país de la tienda en la que desea buscar.
6. Haga clic en **Buscar**.
7. En los resultados de búsqueda, haga clic en **Agregar** para agregar una aplicación.
8. Para filtrar las aplicaciones en la lista de aplicaciones por categoría y para organizar las aplicaciones en categorías en la lista de aplicaciones de trabajo de los dispositivos de los usuarios, puede seleccionar una categoría para la aplicación. En la lista desplegable **Categoría**, realice una de las acciones siguientes:

Opción	
Seleccione una categoría para la aplicación	**a.** En la lista desplegable, seleccione una categoría.
Cree una categoría para la aplicación	**a.** Escriba un nombre para la categoría. La "nueva categoría" aparecerá en la lista desplegable con la etiqueta "nueva categoría" a su lado **b.** Pulse **Intro**. **c.** Pulse **Intro**.

9. En la lista desplegable **Valoración y comentarios de aplicaciones**, realice una de las siguientes acciones. Cuando existen varias versiones de la aplicación, se aplica la configuración especificada a todas las versiones de la aplicación.
   - Si desea que los usuarios valoren y proporcionen comentarios de las aplicaciones y consulten todos los comentarios enviados por otros usuarios en su entorno, seleccione **Modo público**.

- Si desea que los usuarios solo valoren y proporcionen comentarios de aplicaciones, seleccione **Modo privado**. Los usuarios no pueden ver los comentarios proporcionados por otros usuarios. Puede ver comentarios en la consola de gestión de BlackBerry UEM.
- Si no desea que los usuarios valoren o proporcionen comentarios de aplicaciones ni vean los comentarios proporcionados por otros usuarios, seleccione **Desactivado**.

10. En la lista desplegable **Factor de forma compatible con el dispositivo**, seleccione los factores de forma en los que puede instalarse la aplicación. Por ejemplo, puede evitar que la aplicación esté disponible en la aplicación Aplicaciones de trabajo para iPad.
11. Si desea que la aplicación se elimine del dispositivo cuando el dispositivo se haya eliminado de BlackBerry UEM, seleccione **Eliminar la aplicación del dispositivo cuando este se haya eliminado de BlackBerry UEM**. Esta configuración se aplica únicamente cuando la disposición de la aplicación se establece como obligatoria y la opción de instalación predeterminada para las aplicaciones obligatorias se establece en prompt once.
12. Si desea evitar que las aplicaciones en dispositivos iOS realicen la copia de seguridad en el servicio en línea iCloud, seleccione **Desactivar copia de seguridad en iCloud para la aplicación**. Esta opción se aplica únicamente cuando la disposición de la aplicación se establece como obligatoria. La disposición de la aplicación se establece al asignarse a un usuario o grupo.
13. En la lista desplegable **Instalación predeterminada para las aplicaciones obligatorias**, lleve a cabo una de las siguientes acciones:

    - Si desea que los usuarios reciban una solicitud para instalar la aplicación en sus dispositivos iOS, seleccione **Preguntar una vez**. Si los usuarios descartan la solicitud, pueden instalar la aplicación más adelante mediante la pantalla de aplicaciones de trabajo en la aplicación BlackBerry UEM Client o en el icono Aplicaciones de trabajo del dispositivo.
    - Si no desea que los usuarios reciban una solicitud, seleccione **No preguntar**.

    El método de instalación predeterminado se aplica únicamente cuando la disposición de la aplicación se establece como obligatoria. La disposición de la aplicación se establece al asignarse a un usuario o grupo.
14. En la lista desplegable **Convertir aplicación personal instalada en aplicación de trabajo**, seleccione una de las siguientes opciones:

    - Para convertir la aplicación en una aplicación de trabajo si ya está instalada en los dispositivos con iOS 9 o posterior, seleccione **Convertir**. Después de asignar la aplicación a un usuario, la aplicación se convierte en una aplicación de trabajo y se puede administrar con BlackBerry UEM.
    - Si no desea convertir la aplicación en una aplicación de trabajo si ya está instalada en los dispositivos con iOS 9 o versiones posteriores, seleccione **No convertir**. Después de asignar la aplicación a un usuario, BlackBerry UEM no puede administrar la aplicación.
15. Si la configuración de la aplicación se puede preconfigurar (por ejemplo, la información de conexión), y desea hacerlo, obtenga los detalles de configuración del proveedor de la aplicación y lleve a cabo las acciones siguientes:

    a) En la tabla **Configuración de la aplicación**, lleve a cabo una de las tareas siguientes:

Tarea	Pasos
Crear una configuración de la aplicación a partir de una plantilla XML	1. Haga clic en + > **Crear a partir de una plantilla**. 2. Haga clic en **Examinar** y seleccione la plantilla que desea agregar. 3. Haga clic en **Cargar**. 4. Para cada configuración, escriba el valor que desea establecer. Para obtener más información acerca de las plantillas .xml de configuración de aplicaciones, visite http://www.appconfig.org/ios/.
Copiar otra configuración de aplicación	1. Haga clic en + > **Copiar desde una configuración de aplicación**. 2. En la lista desplegable **Copiar desde**, seleccione la configuración de la aplicación que desea copiar. 3. Para cada configuración, edite el valor o nombre de la clave.
Crear una configuración de la aplicación de forma manual	1. Haga clic en + > **Configurar manualmente**. 2. Para cada configuración que desee agregar, haga clic en + y seleccione un tipo de valor para la configuración. 3. Para cada configuración, introduzca el valor o nombre de la clave que desea establecer.

b) Escriba un nombre en el campo **Nombre de configuración de la aplicación**.
c) Haga clic en **Guardar**.
d) Si es necesario, utilice las flechas para mover los perfiles hacia arriba o hacia abajo en la clasificación. Cuando se asigna una aplicación más de una vez con diferentes configuraciones de la aplicación, se aplica la configuración de la aplicación con el rango superior.

16. Haga clic en **Agregar**.

Tareas relacionadas

Asignación de una aplicación a un grupo de usuarios
Asignación de una aplicación a una cuenta de usuario

Adición de una aplicación de Android a la lista de aplicaciones si BlackBerry UEM no está configurado para dispositivos Android Enterprise

Agregue solo aplicaciones a la lista de aplicaciones. Las películas, la música y los quioscos multimedia no se pueden entregar a los dispositivos. Si asigna elementos multimedia a un usuario y configura la disposición de los elementos multimedia como obligatoria, el dispositivo está sujeto a la acción de cumplimiento definida en el perfil de cumplimiento que se le ha asignado.

Si BlackBerry UEM se ha configurado para admitir los dispositivos Android Enterprise, consulte Adición de una aplicación de Android a la lista de aplicaciones si BlackBerry UEM está configurado para Android Enterprise.

1. En la barra de menú, haga clic en **Aplicaciones**.
2. Haga clic en .
3. Haga clic en **Google Play**.
4. Haga clic en **Abrir Google Play** y busque la aplicación que desea agregar. A continuación, puede copiar y pegar información de Google Play en los siguientes pasos y también descargar iconos y capturas de pantalla.
5. En el campo **Nombre de aplicación**, escriba el nombre de la aplicación.
6. En el campo **Descripción de la aplicación**, escriba una descripción para la aplicación.
7. Para filtrar las aplicaciones en la lista de aplicaciones por categoría y para organizar las aplicaciones en categorías en la lista de aplicaciones de trabajo de los dispositivos de los usuarios, puede seleccionar una categoría para la aplicación. En la lista desplegable **Categoría**, realice una de las acciones siguientes:

Opción	
Seleccione una categoría para la aplicación	**a.** En la lista desplegable, seleccione una categoría.
Cree una categoría para la aplicación	**a.** Escriba un nombre para la categoría. La "nueva categoría" aparecerá en la lista desplegable con la etiqueta "nueva categoría" a su lado **b.** Pulse **Intro**. **c.** Pulse **Intro**.

8. En la lista desplegable **Valoración y comentarios de aplicaciones**, realice una de las siguientes acciones. Cuando existen varias versiones de la aplicación, se aplica la configuración especificada a todas las versiones de la aplicación.
   - Si desea que los usuarios valoren y proporcionen comentarios de las aplicaciones y consulten todos los comentarios enviados por otros usuarios en su entorno, seleccione **Modo público**.
   - Si desea que los usuarios solo valoren y proporcionen comentarios de aplicaciones, seleccione **Modo privado**. Los usuarios no pueden ver los comentarios proporcionados por otros usuarios. Puede ver comentarios en la consola de gestión de BlackBerry UEM.
   - Si no desea que los usuarios valoren o proporcionen comentarios de aplicaciones ni vean los comentarios proporcionados por otros usuarios, seleccione **Desactivado**.
9. En el campo **Proveedor**, escriba el nombre del proveedor de la aplicación.
10. En el campo **Icono de la aplicación**, haga clic en **Examinar**. Localice y seleccione un icono para la aplicación. Los formatos compatibles son .png, .jpg, .jpeg o .gif. No utilice Google Chrome para descargar el icono porque se descarga una imagen .webp incompatible.
11. En el campo **Dirección web de la aplicación de Google Play**, escriba la dirección web de la aplicación en Google Play.
12. Para agregar las capturas de pantalla de la aplicación, haga clic en **Agregar** y busque las capturas de pantalla. Los tipos de imagen compatibles son .jpg, .jpeg, .png, o .gif.
13. En la lista desplegable **Enviar a**, lleve a cabo una de las acciones siguientes:
    - Si desea enviar la aplicación a todos los dispositivos Android, seleccione **Todos los dispositivos Android**.
    - Si desea enviar la aplicación únicamente a los dispositivos Android que utilicen Samsung KNOX Workspace, seleccione **Solo dispositivos con KNOX Workspace**.
14. Haga clic en **Agregar**.

Tareas relacionadas

Asignación de una aplicación a un grupo de usuarios
Asignación de una aplicación a una cuenta de usuario

Adición de una aplicación de Android a la lista de aplicaciones si BlackBerry UEM está configurado para Android Enterprise

Si ha configurado la compatibilidad con activaciones de Android Enterprise, la conexión a Google que ha configurado permite a BlackBerry UEM obtener la información de la aplicación de Google Play. La conexión a Google Play se realiza directamente desde el ordenador que ejecuta la consola de BlackBerry UEM. Si su empresa está utilizando un servidor proxy, debe asegurarse de que no se produzca intercepción de SSL. Para obtener más información sobre los puertos que deben estar abiertos, visite support.blackberry.com para leer el artículo KB52777. Para obtener más información sobre la configuración de BlackBerry UEM para admitir dispositivos Android Enterprise, consulte el contenido de Configuración.

Si BlackBerry UEM no se ha configurado para admitir los perfiles de trabajo de Android, consulte Adición de una aplicación de Android a la lista de aplicaciones si BlackBerry UEM no está configurado para dispositivos Android Enterprise.

Para utilizar Google Play para administrar aplicaciones en Samsung KNOX Workspace, los dispositivos deben tener instalado Samsung KNOX 2.7.1 o posterior y debe permitir la administración de aplicaciones de Google Play para dispositivos Samsung KNOX Workspace en el perfil de activación.

Nota: En una futura versión de BlackBerry UEM, la configuración aplicable a BlackBerry Hub + y Divide Productivity se eliminará del perfil de correo y solo estará disponible como una configuración de la aplicación en los ajustes de la misma. En dicha versión, si configura los ajustes de la aplicación en el perfil de correo y en la configuración de la aplicación, esta última tendrá prioridad si ambas están asignadas.

1. En la barra de menú, haga clic en **Aplicaciones**.
2. Haga clic en .
3. Haga clic en **Google Play**.
4. Busque la aplicación que desea agregar o seleccione una aplicación en la página de inicio de la tienda.
5. Seleccione la aplicación.
6. Haga clic en **Aprobar**.
7. Para aceptar permisos de aplicación en nombre de los usuarios, haga clic **Aprobar**. Debe aceptar los permisos de aplicaciones para permitir que las aplicaciones obligatorias se instalen automáticamente en los dispositivos Android con un perfil de trabajo o en KNOX Workspace. Si no acepta los permisos de aplicaciones en nombre de los usuarios, las aplicaciones no se pueden administrar en BlackBerry UEM.
8. En la pestaña **Ajustes de aprobación**, elija cómo desea gestionar las nuevas solicitudes de permisos de aplicación cuando hay una aplicación actualizada.
   - Para aceptar automáticamente los nuevos permisos añadidos por el proveedor de la aplicación, seleccione **Mantener aprobación cuando la aplicación solicite nuevos permisos**.
   - Para volver a aceptar manualmente los nuevos permisos de aplicación del proveedor de la aplicación antes de que la aplicación se envíe a los nuevos dispositivos, seleccione **Revocar aprobación de la aplicación cuando esta aplicación solicite nuevos permisos**. Para obtener más información acerca de la actualización de los permisos de aplicación, consulte Actualizar permisos de aplicaciones para aplicaciones con perfiles de trabajo de Android.
9. Si ha seleccionado la opción **Revocar aprobación de la aplicación cuando esta aplicación solicite nuevos permisos**, en la pestaña Notificaciones, agregue un suscriptor para notificarlo cuando el permiso de la aplicación cambie. El administrador tendrá que volver a aprobar la aplicación para que los usuarios puedan acceder a ella.
10. Haga clic en **Guardar**.

11. En el campo **Descripción de la aplicación**, escriba una descripción para la aplicación.
12. Para agregar las capturas de pantalla de la aplicación, haga clic en **Agregar** y busque las capturas de pantalla. Los tipos de imagen compatibles son .jpg, .jpeg, .png, o .gif.
13. En la lista desplegable **Enviar a**, lleve a cabo una de las acciones siguientes:
    - Si desea enviar la aplicación a todos los dispositivos Android, seleccione **Todos los dispositivos Android**.
    - Si desea enviar la aplicación únicamente a los dispositivos Android que utilicen Samsung KNOX Workspace, seleccione **Dispositivos Samsung KNOX Workspace**.
    - Si desea que la aplicación se envíe únicamente a dispositivos Android con un perfil de trabajo, seleccione **Dispositivos Android con un perfil de trabajo**.
14. Para las aplicaciones compatibles con los ajustes de la configuración, se muestra la tabla **Configuración de la aplicación**. Si desea crear una configuración de la aplicación, realice los pasos siguientes:
    a) Haga clic en + para agregar un ID de paquete de aplicación.
    b) Escriba un nombre para la configuración de la aplicación y especifique los valores de configuración que utilizar.
    c) Haga clic en **Guardar**.
    d) Si es necesario, utilice las flechas para mover los perfiles hacia arriba o hacia abajo en la clasificación. Cuando se asigna una aplicación más de una vez con diferentes configuraciones de la aplicación, se aplica la configuración de la aplicación con el rango superior.
15. Para filtrar las aplicaciones en la lista de aplicaciones por categoría y para organizar las aplicaciones en categorías en la lista de aplicaciones de trabajo de los dispositivos de los usuarios, puede seleccionar una categoría para la aplicación. En la lista desplegable **Categoría**, realice una de las acciones siguientes:

Opción	
Seleccione una categoría para la aplicación	**a.** En la lista desplegable, seleccione una categoría.
Cree una categoría para la aplicación	**a.** Escriba un nombre para la categoría. La nueva categoría aparecerá en la lista desplegable con la etiqueta "nueva categoría" a su lado **b.** Pulse **Intro**. **c.** Pulse **Intro**.

16. En la lista desplegable **Valoración y comentarios de aplicaciones**, realice una de las siguientes acciones. Cuando existen varias versiones de la aplicación, se aplica la configuración especificada a todas las versiones de la aplicación.
    - Si desea que los usuarios valoren y proporcionen comentarios de las aplicaciones y consulten todos los comentarios enviados por otros usuarios en su entorno, seleccione **Modo público**.
    - Si desea que los usuarios solo valoren y proporcionen comentarios de aplicaciones, seleccione **Modo privado**. Los usuarios no pueden ver los comentarios proporcionados por otros usuarios. Puede ver comentarios en la consola de gestión de BlackBerry UEM.
    - Si no desea que los usuarios valoren o proporcionen comentarios de aplicaciones ni vean los comentarios proporcionados por otros usuarios, seleccione **Desactivado**.
17. Haga clic en **Agregar**.

Tareas relacionadas

Asignación de una aplicación a un grupo de usuarios
Asignación de una aplicación a una cuenta de usuario

Adición de una aplicación Windows Phone a la lista de aplicaciones

1. En la barra de menús, haga clic en **Aplicaciones**.
2. Haga clic en .
3. Haga clic en **Tienda Windows** > **8**.
4. Haga Clic en **Abrir Tienda Windows** y busque la aplicación que desea agregar. A continuación, puede copiar y pegar información de la Windows Store en los siguientes pasos y también descargar iconos y capturas de pantalla.
5. En el campo **Nombre de aplicación**, escriba el nombre de la aplicación.
6. En el campo **Descripción de la aplicación**, escriba una descripción para la aplicación.
7. En la lista desplegable **Valoración y comentarios de aplicaciones**, realice una de las siguientes acciones. Cuando existen varias versiones de la aplicación, se aplica la configuración especificada a todas las versiones de la aplicación.
   - Si desea que los usuarios valoren y proporcionen comentarios de las aplicaciones y consulten todos los comentarios enviados por otros usuarios en su entorno, seleccione **Modo público**.
   - Si desea que los usuarios solo valoren y proporcionen comentarios de aplicaciones, seleccione **Modo privado**. Los usuarios no pueden ver los comentarios proporcionados por otros usuarios. Puede ver comentarios en la consola de gestión de BlackBerry UEM.
   - Si no desea que los usuarios valoren o proporcionen comentarios de aplicaciones o vean los comentarios proporcionados por otros usuarios, seleccione **Desactivado**.
8. En el campo **Proveedor**, escriba el nombre del proveedor de la aplicación.
9. En el campo **Icono de la aplicación**, haga clic en **Examinar**. Localice y seleccione un icono para la aplicación. Los formatos compatibles son .png, .jpg, .jpeg o .gif.
10. En el campo **Dirección web de la aplicación de la Tienda Windows**, escriba la dirección web de la aplicación en la Windows Store. La dirección web debe empezar por https.
11. Para agregar las capturas de pantalla de la aplicación, haga clic en **Agregar** y busque las capturas de pantalla. Los tipos de imagen compatibles son .jpg, .jpeg, .png, o .gif.
12. Haga clic en **Agregar**.

Adición de una aplicación Windows 10 a la lista de aplicaciones

Para agregar aplicaciones de Windows 10 a la lista de aplicaciones, debe administrar su catálogo de aplicaciones a través de la Tienda Windows Store para empresas y, a continuación, sincronizar las aplicaciones con BlackBerry UEM. Cuando se agregan nuevas aplicaciones al catálogo de aplicaciones, puede sincronizarlas con BlackBerry UEM en el momento o esperar que BlackBerry UEM se sincronice automáticamente. BlackBerry UEM sincroniza el catálogo de aplicaciones cada 24 horas.

Puede permitir que los usuarios instalen aplicaciones en línea y sin conexión de la Tienda Windows Store para el catálogo de aplicaciones de empresas. BlackBerry UEM descarga las aplicaciones sin conexión cuando realiza una sincronización con el catálogo de aplicaciones. Se recomienda el uso de las aplicaciones sin conexión ya que toda la administración de dichas aplicaciones se puede realizar desde BlackBerry UEM, y los usuarios pueden instalarlas sin tener que conectarse a la Windows Store para empresas. Una vez instaladas las aplicaciones, los dispositivos reciben actualizaciones para las aplicaciones desde la Windows Store.

Las aplicaciones en línea se descargan directamente de la Tienda Windows Store para empresas. Para poder enviar las aplicaciones en línea necesarias a los dispositivos, indique a los usuarios que agreguen sus cuentas de trabajo a **Cuentas utilizadas por otras aplicaciones** en Windows 10.

Antes de empezar:

- Especificación de la ubicación de red compartida para guardar aplicaciones internas para almacenar aplicaciones sin conexión.
- Configure BlackBerry UEM para que se sincronice con la Tienda Windows Store para empresas. Para obtener más instrucciones, consulte el contenido de Configuración.

1. En la barra de menú, haga clic en **Aplicaciones**.
2. Haga clic en .
3. Haga clic en **Tienda Windows** > **10**.
4. Haga clic en **Sincronizar aplicaciones**.

Permiso para que los usuarios instalen aplicaciones Windows 10 en línea

Para permitir que los usuarios instalen aplicaciones Windows 10 en línea, el usuario debe existir en su directorio de Microsoft Azure y la dirección de correo del usuario en BlackBerry UEM debe coincidir con la de Microsoft Azure AD. Puede sincronizar el directorio con Microsoft Azure mediante el uso de Microsoft Azure AD Connect. Para obtener más instrucciones, consulte el contenido de Configuración.

Nota: Para poder enviar las aplicaciones en línea necesarias a los dispositivos, indique a los usuarios que agreguen sus cuentas de trabajo a **Cuentas utilizadas por otras aplicaciones** en Windows 10.

Agregue una categoría de aplicación para una aplicación de Windows 10

Una vez que configure una categoría para una aplicación, puede filtrar las aplicaciones en la lista de aplicaciones por categoría y organizar las aplicaciones de la lista de aplicaciones de trabajo en los dispositivos de los usuarios por categorías. Después de haber sincronizado una aplicación de Windows 10 con BlackBerry UEM, puede asignarle una categoría de aplicación.

Antes de empezar: Adición de una aplicación Windows 10 a la lista de aplicaciones.

1. En la barra de menú, haga clic en **Aplicaciones**.
2. Haga clic la aplicación a la que desee asignar una categoría de aplicación.
3. En la lista desplegable **Categoría**, realice una de las acciones siguientes:

Paso	Descripción
Seleccione una categoría para la aplicación	**a.** En la lista desplegable, seleccione una categoría.
Cree una categoría para la aplicación	**a.** Escriba un nombre para la categoría. Aparecerá un mensaje de "nueva categoría" en la lista desplegable con la etiqueta "nueva categoría" a su lado. **b.** Pulse **Enter (Intro)**. **c.** Pulse **Enter (Intro)**.

4. Haga clic en **Guardar**.

Adición de aplicaciones públicas de BlackBerry Dynamics a la lista de aplicaciones

Para agregar aplicaciones públicas de BlackBerry Dynamics a la lista de aplicaciones en BlackBerry UEM, su empresa debe estar autorizada para utilizar aplicaciones en BlackBerry Marketplace for Enterprise Software. BlackBerry Marketplace for Enterprise Software contiene un catálogo de aplicaciones de BlackBerry Dynamics. Después de que la organización obtenga la autorización para utilizar la aplicación, puede actualizar la lista

de aplicaciones para sincronizar las aplicaciones con BlackBerry UEM inmediatamente o esperar hasta que BlackBerry UEM realice la sincronización automáticamente. BlackBerry UEM sincroniza las aplicaciones de BlackBerry Dynamics cada 24 horas.

Nota: Los usuarios deben activar las aplicaciones dinámicas en el mismo entorno de BlackBerry UEM desde el que se han asignado las aplicaciones. No es posible activar aplicaciones de BlackBerry Dynamics desde un entorno de BlackBerry Dynamics externo.

1. Inicie sesión en su cuenta en https://apps.good.com/pce/#/apps.
2. Busque la aplicación en BlackBerry Marketplace for Enterprise Software y solicite una versión de prueba. La aplicación estará disponible para su empresa y se puede asignar a los usuarios después de que la aplicación se haya sincronizado con BlackBerry UEM.
3. Para comprar la aplicación, siga las instrucciones proporcionadas por el desarrollador de la aplicación.

Después de terminar:

- Actualice la lista de aplicaciones para sincronizar aplicaciones con BlackBerry UEM.

Visualización de autorizaciones de aplicaciones públicas de BlackBerry Dynamics

1. Inicie sesión en https://account.good.com/pce/#/a/organization//servers.
2. Expanda **Autorizaciones**.

Adición de aplicaciones internas a la lista de aplicaciones

Las aplicaciones internas incluyen aplicaciones propias desarrolladas por la empresa o aplicaciones disponibles para uso exclusivo de la empresa. Las aplicaciones internas no se agregan desde tiendas de aplicaciones públicas.

Las aplicaciones de BlackBerry deben ser archivos .bar, las aplicaciones de iOS deben ser archivos .ipa, las aplicaciones de Android deben ser archivos .apk y las aplicaciones de Windows Phone deben ser archivos .xap o archivos .appx. Las aplicaciones internas también deben estar firmadas e inalteradas.

Los usuarios pueden buscar aplicaciones internas en los dispositivos como se indica a continuación:

- Para los dispositivos con BlackBerry 10, en la pestaña Aplicaciones de empresa de BlackBerry World for Work
- Para los dispositivos iOS, Android y Windows Phone, en la lista Aplicaciones de trabajo asignadas en la aplicación BlackBerry UEM Client

Pasos para agregar aplicaciones internas a la lista de aplicaciones

Al agregar aplicaciones internas, realice las acciones siguientes:

Paso	Acción
1	Especificación de la ubicación de red compartida para guardar aplicaciones internas.
2	Si agrega aplicaciones de Windows Phone, cargue un AET.
3	Si la aplicación no es una aplicación de BlackBerry Dynamics, agregue una aplicación interna a la lista de aplicaciones.

Paso	Acción
4	Si la aplicación es una aplicación de BlackBerry Dynamics, agregue una autorización de aplicaciones de BlackBerry Dynamics interna y luego cargue los archivos de origen de las aplicaciones de BlackBerry Dynamics.
5	Si va a agregar una aplicación interna que desea tener disponible en los dispositivos Android que utilizan un perfil de trabajo, realice los pasos para alojar la aplicación en Google Play o en BlackBerry UEM.

Especificación de la ubicación de red compartida para guardar aplicaciones internas

Antes de agregar aplicaciones internas a la lista de aplicaciones disponibles, debe especificar una ubicación de red compartida para guardar los archivos de origen de la aplicación. Para asegurarse de que las aplicaciones internas sigan disponibles, esta ubicación de red debe tener una solución de alta disponibilidad y realizar copias de seguridad periódicamente. Asimismo, no cree la carpeta de red compartida en la carpeta de instalación de BlackBerry UEM porque se eliminará si actualiza BlackBerry UEM.

Antes de empezar:

- Cree una carpeta de red compartida para guardar los archivos de origen de aplicaciones internas en la red en la que se aloja BlackBerry UEM.
- Compruebe que la cuenta de servicios para el equipo que aloja BlackBerry UEM tiene acceso de lectura y escritura a la carpeta de red compartida.

1. En la barra de menú, haga clic en **Configuración**.
2. En el panel izquierdo, amplíe **Administración de aplicaciones**.
3. Haga clic en **Almacenamiento de aplicaciones internas**.
4. En el campo de **Ubicación de la red**, escriba la ruta de la carpeta de red compartida mediante el siguiente formato:

   \\<*nombre_ordenador*>\<*carpeta_red_compartida*>

   La ruta de la red compartida debe escribirse en formato UNC (por ejemplo: \\NombreEquipo\Aplicaciones\AplicacionesInternas).
5. Haga clic en **Guardar**.

Carga de un identificador de inscripción de la aplicación para los dispositivos Windows Phone

Un AET debe cargarse antes de que los usuarios puedan instalar aplicaciones internas en dispositivos Windows Phone. Las aplicaciones que desea que los usuarios instalen deben compartir un certificado con el AET que haya cargado. Para obtener más información acerca de cómo generar un identificador de inscripción de la aplicación, visite msdn.microsoft.com y consulte el artículo *Cómo generar un identificador de inscripción de la aplicación para Windows Phone*. También necesitará un AET si desea controlar aplicaciones Windows internas o públicas en los perfiles de cumplimiento.

1. En la barra de menú, haga clic en **Configuración**.
2. En el panel izquierdo, amplíe **Administración de aplicaciones**.
3. Haga clic en **Aplicaciones de Windows Phone**.
4. Haga clic en **Examinar** y busque el AET que desea agregar o actualizar.
5. Haga clic en **Guardar**.

Adición de una aplicación interna a la lista de aplicaciones

Antes de empezar:

- Especificación de la ubicación de red compartida para guardar aplicaciones internas.
- Si agrega aplicaciones de Windows Phone, cargue un AET.

1. En la barra de menú, haga clic en **Aplicaciones**.
2. Haga clic en .
3. Haga clic en **Aplicaciones internas**.
4. Haga clic en **Examinar**. Busque la aplicación que desea agregar o actualizar.
5. Haga clic en **Abrir**.
6. Haga clic en **Agregar**.
7. Opcionalmente, puede agregar un nombre de proveedor y una descripción de la aplicación.
8. Para agregar capturas de pantalla de la aplicación, haga clic en **Agregar**. Busque las capturas de pantalla. Los tipos de imagen compatibles son .jpg, .jpeg, .png, o .gif.
9. Para filtrar las aplicaciones en la lista de aplicaciones por categoría y para organizar las aplicaciones en categorías en la lista de aplicaciones de trabajo de los dispositivos de los usuarios, puede seleccionar una categoría para la aplicación. En la lista desplegable **Categoría**, realice una de las acciones siguientes:

Opción	
Seleccione una categoría para la aplicación	**a.** En la lista desplegable, seleccione una categoría.
Cree una categoría para la aplicación	**a.** Escriba un nombre para la categoría. La "nueva categoría" aparecerá en la lista desplegable con la etiqueta "nueva categoría" a su lado **b.** Pulse **Intro**. **c.** Pulse **Intro**.

10. En la lista desplegable **Valoración y comentarios de aplicaciones**, realice una de las siguientes acciones. Cuando existen varias versiones de la aplicación, se aplica la configuración especificada a todas las versiones de la aplicación.
    - Si desea que los usuarios valoren y proporcionen comentarios de las aplicaciones y consulten todos los comentarios enviados por otros usuarios en su entorno, seleccione **Modo público**.
    - Si desea que los usuarios solo valoren y proporcionen comentarios de aplicaciones, seleccione **Modo privado**. Los usuarios no pueden ver los comentarios proporcionados por otros usuarios. Puede ver comentarios en la consola de gestión de BlackBerry UEM.
    - Si no desea que los usuarios valoren o proporcionen comentarios de aplicaciones o vean los comentarios proporcionados por otros usuarios, seleccione **Desactivado**.
11. Si agrega una aplicación de iOS, realice las siguientes acciones:
    a) En la lista desplegable **Factor de forma compatible con el dispositivo**, seleccione los factores de forma en los que puede instalarse la aplicación. Por ejemplo, puede evitar que la aplicación esté disponible en la aplicación Aplicaciones de trabajo para iPad.
    b) Si desea que la aplicación se elimine del dispositivo cuando el dispositivo se haya eliminado de BlackBerry UEM, seleccione **Eliminar la aplicación del dispositivo cuando este se haya eliminado de BlackBerry UEM**. Esta configuración se aplica únicamente cuando la disposición de la aplicación se establece como obligatoria y la opción de instalación predeterminada para las aplicaciones obligatorias se establece en prompt once.
    c) Si desea evitar que las aplicaciones en dispositivos iOS realicen la copia de seguridad en el servicio en línea iCloud, seleccione **Desactivar copia de seguridad en iCloud para la aplicación**. Esta opción se aplica

únicamente cuando la disposición de la aplicación se establece como obligatoria. La disposición de la aplicación se establece al asignarse a un usuario o grupo.

d) En la lista desplegable **Método de instalación predeterminado para las aplicaciones obligatorias**, si desea que los usuarios reciban una solicitud para instalar la aplicación en sus dispositivos iOS, seleccione **Preguntar una vez**. Si los usuarios descartan la solicitud, pueden instalar la aplicación más adelante mediante la lista Aplicaciones de trabajo en la aplicación BlackBerry UEM Client o en el icono Aplicaciones de trabajo del dispositivo.

12. Si agrega una aplicación de Android, en la lista desplegable **Enviar a**, lleve a cabo una de las acciones siguientes:
    - Si desea enviar la aplicación a todos los dispositivos Android, seleccione **Todos los dispositivos Android**.
    - Si desea enviar la aplicación únicamente a los dispositivos Android que utilicen Samsung KNOX Workspace, seleccione **Dispositivos Samsung KNOX Workspace**.
    - Si desea que la aplicación se envíe únicamente a dispositivos Android con un perfil de trabajo, seleccione **Dispositivos Android con un perfil de trabajo**.
13. Para permitir que se instale la aplicación en dispositivos Android con un perfil de trabajo, seleccione **Permitir la aplicación para perfiles de trabajo**.
14. Para las aplicaciones compatibles con los ajustes de la configuración, se muestra la tabla **Configuración de la aplicación**. Haga clic en + para agregar una configuración de la aplicación. Para obtener más información, consulte Adición o cambio de la configuración de la aplicación.
15. Haga clic en **Agregar**. Si planea alojar la aplicación en BlackBerry UEM mediante un archivo .json,, copie y guarde la URL que se muestra.

Después de terminar: Si selecciona la opción **Permitir la aplicación para perfiles de trabajo de Android**, realice una de las siguientes tareas:

- Organice una aplicación interna para dispositivos Android con un perfil de trabajo en Google Play utilizando un archivo .apk
- Organice una aplicación interna para dispositivos Android con un perfil de trabajo en BlackBerry UEM utilizando un archivo .json

Adición de una autorización de aplicaciones internas de BlackBerry Dynamics

Para agregar una aplicación interna de BlackBerry Dynamics, debe agregar una autorización. Después de agregar la autorización, puede cargar los archivos de origen de la aplicación.

Antes de empezar:

- Especificación de la ubicación de red compartida para guardar aplicaciones internas.
- Si agrega aplicaciones de Windows Phone, cargue un AET.
- Debe tener una licencia de Application Edition o Content Edition para poder añadir una autorización de aplicaciones internas de BlackBerry Dynamics

1. En la barra de menú, haga clic en **Aplicaciones**.
2. Haga clic en .
3. Haga clic en **Autorizaciones de aplicaciones internas de BlackBerry Dynamics**.
4. En el campo Nombre, escriba el nombre de la aplicación que desee agregar.
5. En el campo **ID de autorización de BlackBerry Dynamics**, introduzca el ID de autorización de la aplicación que desee agregar. Si no sabe el ID de autorización de la aplicación, póngase en contacto con el desarrollador de la aplicación. Para obtener más información sobre los ID de autorización, consulte la documentación de BlackBerry Dynamics SDK. El ID de autorización debe estar en el siguiente formato:
    - Nombre del dominio al revés, por ejemplo, `com.yourcompany.appname`.
    - No puede comenzar de ninguna de las siguientes formas

    - com.blackberry
    - com.good
    - com.rim
    - net.rim
  - No puede contener letras en mayúsculas.
  - Debe cumplir con el formato <subdominio> definido en la sección 2.3.1 de RFC 1035, modificado por la sección 2.1 de RFC 1123.
6. En el campo **Versión de autorización de BlackBerry Dynamics**, introduzca la versión de autorización. Si no sabe la versión de autorización de la aplicación, póngase en contacto con el desarrollador de la aplicación. La versión de autorización debe estar en el siguiente formato:
   - Desde uno hasta cuatro segmentos de dígitos, separados por puntos, por ejemplo, 100 o 1.2.3.4.
   - Sin ceros a la izquierda en segmentos numéricos. Por ejemplo, no puede utilizar 0100 o 01.02.03.04.
   - La longitud de los segmentos numéricos puede ser desde uno hasta tres caracteres, por ejemplo, 100.200.300.400.
7. De manera opcional, agregue una descripción de la aplicación.
8. Haga clic en **Agregar**.

Después de terminar:

- Carga de archivos de origen de las aplicaciones de BlackBerry Dynamics
- Para acceder a las aplicaciones que se instalarán en los dispositivos Android que utilizan un perfil de trabajo, realice una de las siguientes tareas:
  - Organice una aplicación interna para dispositivos con un perfil de trabajo de Android en Google Play utilizando un archivo .apk
  - Organice una aplicación interna para dispositivos Android con un perfil de trabajo en BlackBerry UEM utilizando un archivo .json

Carga de archivos de origen de las aplicaciones de BlackBerry Dynamics

Una vez que se haya creado una autorización de aplicaciones de BlackBerry Dynamics, puede cargar los archivos de origen para las plataformas aplicables de los dispositivos.

Nota: Los usuarios deben activar las aplicaciones dinámicas en el mismo entorno de BlackBerry UEM desde el que se han asignado las aplicaciones. No es posible activar aplicaciones de BlackBerry Dynamics desde un entorno de BlackBerry Dynamics externo.

Antes de empezar:

- Adición de una autorización de aplicaciones internas de BlackBerry Dynamics

1. En la barra de menú, haga clic en **Aplicaciones**.
2. Haga clic en la aplicación para la que desea cargar los archivos de origen.
3. Haga clic en la pestaña de la plataforma del dispositivo para la que desea cargar un archivo de origen.
4. En la sección **Archivo de origen de aplicación**, haga clic en **Agregar**.
5. Haga clic en **Examinar**. Busque la aplicación que desea agregar o actualizar.
6. Haga clic en **Agregar**.
7. Si es necesario, actualice la configuración de las aplicaciones. Para obtener más información, consulte Gestión de la configuración de una aplicación de BlackBerry Dynamics.

Organice una aplicación interna para dispositivos Android con un perfil de trabajo en Google Play utilizando un archivo .apk

Cuando se aloja una aplicación en Google Play, se pueden utilizar ajustes de configuración para modificar los comportamientos de las aplicaciones y establecer la aplicación como obligatoria u opcional. Para alojar una aplicación en Google Play, debe publicar la aplicación en Google Play de modo que los usuarios puedan instalar la aplicación interna en sus dispositivos.

Antes de empezar:

- En BlackBerry UEM, agregue el archivo .apk interno a la lista de aplicaciones. Seleccione la opción **Permitir la aplicación para Android for Work** y, en la lista desplegable **La aplicación se ofrecerá en**, haga clic en **Google Play**.
  Nota: Debe seleccionar **Permitir la aplicación para perfiles de trabajo de Android** incluso si aloja la aplicación para todos los dispositivos Android.
- Necesita una cuenta para iniciar sesión en Google Developers Console. Si se ha configurado un perfil de trabajo de Android, debe utilizar la misma dirección de correo para la cuenta de desarrollador que utilizó para configurar. Para cada dominio de BlackBerry UEM necesita otra cuenta de desarrollador.

Visite https://support.blackberry.com/kb para leer el artículo 47873 y obtener instrucciones sobre el alojamiento de una aplicación interna para dispositivos Android con un perfil de trabajo en BlackBerry UEM utilizando un archivo .apk.

Tareas relacionadas

Adición de una aplicación interna a la lista de aplicaciones

Organice una aplicación interna para dispositivos Android con un perfil de trabajo en BlackBerry UEM utilizando un archivo .json

Para alojar una aplicación interna en los dispositivos Android con un perfil de trabajo en BlackBerry UEM, debe generar un archivo .json para la aplicación, cargar el archivo en Google Play y obtener la clave de licencia para la aplicación publicada. Las aplicaciones que se alojan en BlackBerry UEM se pueden establecer únicamente como opcionales y no se pueden utilizar los ajustes de configuración para modificar las características y los comportamientos de las aplicaciones.

Antes de empezar:

- Compruebe que dispone de OpenSSL, JDK, Python 2.x y Android Asset Packaging Tool (aapt) instalados en una ubicación de ruta en el ordenador.
- Necesita una cuenta para iniciar sesión en Google Developers Console. Si ha configurado la compatibilidad con los perfiles de trabajo de Android, utilice la misma dirección de correo electrónico para la cuenta de desarrollador que utilizó para configurar los perfiles de trabajo de Android. Para cada dominio de BlackBerry UEM necesita otra cuenta de desarrollador.
- En BlackBerry UEM, agregue una aplicación interna a la lista de aplicaciones. Seleccione la opción **Permitir la aplicación para perfiles de trabajo de Android** y, en la lista desplegable **La aplicación se ofrecerá en**, haga clic en **BlackBerry UEM**. Copie y guarde la URL que se muestra en BlackBerry UEM.
  Nota: Debe seleccionar **Permitir la aplicación para perfiles de trabajo de Android** incluso si aloja la aplicación para todos los dispositivos Android.

Visite http://support.blackberry.com/kb para leer el artículo 47768 y obtener instrucciones sobre el alojamiento de una aplicación interna para dispositivos Android con un perfil de trabajo en BlackBerry UEM utilizando un archivo .json.

Tareas relacionadas

Adición de una aplicación interna a la lista de aplicaciones

Actualizar una aplicación interna

Al actualizar una aplicación interna, la aplicación actualizada sustituirá a la aplicación asignada actualmente a los usuarios y grupos. Los dispositivos BlackBerry actualizan la versión de la aplicación automáticamente. Otros dispositivos podrían solicitar al usuario que instale la nueva versión de la aplicación.

Antes de empezar: Si va a actualizar una aplicación alojada en Google Play para dispositivos Android con un perfil de trabajo, añada la versión actualizada de la aplicación a Google Play y espere a que Google publique la aplicación antes de actualizarla en BlackBerry UEM.

1. En la barra de menú, haga clic en **Aplicaciones**.
2. Haga clic en la aplicación interna que desea actualizar.
3. En la esquina superior derecha, haga clic en .
4. En el cuadro de diálogo **Actualizar aplicación interna**, haga clic en **Examinar** y vaya a la aplicación que desee actualizar.
5. Haga clic en **Agregar** hasta que aparezca el botón **Guardar**.
6. Haga clic en **Save**.

Actualizar una aplicación interna para dispositivos Android con un perfil de trabajo en BlackBerry UEM utilizando un archivo .json

Visite https://support.blackberry.com/kb para leer el artículo 47768 y obtener instrucciones sobre la actualización de una aplicación interna para dispositivos Android con un perfil de trabajo en BlackBerry UEM utilizando un archivo .json.

Adición o cambio de la configuración de la aplicación

Las configuraciones de la aplicación le permiten preconfigurar los ajustes de aplicaciones determinadas antes de asignar aplicaciones a los usuarios. Mediante la preconfiguración de los ajustes de las aplicaciones, puede hacer que sea más sencillo para los usuarios descargar, configurar y utilizar aplicaciones. Por ejemplo, muchas aplicaciones requieren que los usuarios escriban una URL, una dirección de correo electrónico u otra información antes de poder utilizarlas. Si añade una configuración de la aplicación, puede configurar algunos de estos ajustes de antemano. Puede crear varias configuraciones de la aplicación para una aplicación con diferentes ajustes para distintos fines y clasificar las configuraciones. Si una aplicación se asigna a un usuario más de una vez con diferentes configuraciones de la aplicación, se aplica la aplicación con la clasificación más alta.

En BlackBerry UEM, puede crear una configuración de la aplicación para las siguientes aplicaciones:

- Aplicaciones de iOS (públicas o internas) que se desarrollan con capacidades de configuración gestionadas. Consulte Adición de una aplicación de iOS a la lista de aplicaciones.
- Aplicaciones de Android (públicas o internas) que se desarrollan con capacidades de restricciones de aplicaciones de Android. BlackBerry UEM debe configurarse para que sea compatible con los perfiles de trabajo de Android. Consulte Adición de una aplicación de Android a la lista de aplicaciones si BlackBerry UEM está configurado para Android Enterprise.

Para obtener información acerca de la configuración de aplicaciones, póngase en contacto con el proveedor de la aplicación.

Para obtener más información acerca de la configuración de aplicaciones, visite http://www.appconfig.org/.

Agregar accesos directos de aplicación

Puede utilizar accesos directos de aplicaciones para agregar un acceso directo personalizado al dispositivo o a BlackBerry Dynamics Launcher. Por ejemplo, puede agregar un acceso directo al sitio web interno de su empresa. Para cada acceso directo de aplicación, puede configurar los atributos siguientes:

- La dirección web que se abre cuando los usuarios tocan el icono
- Etiqueta e icono del acceso directo
- Ubicación para agregar el acceso directo de aplicación (por ejemplo, el BlackBerry Dynamics Launcher)
- Si la dirección web se abre en el navegador seguro de BlackBerry Access

Nota: Los perfiles de los iconos web ahora son accesos directos de aplicación. En la versión 12.7 o posterior de BlackBerry UEM, un perfil de icono web de la versión 12.6 o anterior de BlackBerry UEM se convierte automáticamente en un acceso directo de aplicación. Los accesos directos de aplicaciones se pueden encontrar en la lista de aplicaciones en la consola de gestión.

Crear un acceso directo de aplicación

Debe crear un acceso directo de aplicación para cada acceso directo que desea mostrar en los dispositivos de los usuarios. Para los dispositivos activados con BlackBerry Dynamics, tiene la opción de agregar el acceso directo a BlackBerry Dynamics Launcher.

Antes de empezar:

- Compruebe que se ha asignado a los usuarios el derecho de la aplicación para "Función – Tienda de aplicaciones BlackBerry" (com.blackberry.feature.appstore).
- Verifique que la imagen que está pensando utilizar como icono para el acceso directo cumpla los siguientes requisitos:
  - Los formatos de imagen son .png, .jpg, .jpeg.
  - La imagen no tiene elementos transparentes. Los elementos transparentes se mostrarán como negro en el dispositivo.
  - El tamaño máximo de la imagen es 120x120.

1. En la barra de menú, haga clic en **Aplicaciones**.
2. Haga clic en .
3. Haga clic en **Acceso directo de aplicación**.
4. Escriba un nombre y una descripción para el acceso directo de aplicación. El nombre se utiliza como la etiqueta del acceso directo de aplicación.
5. En el campo **Icono del acceso directo**, haga clic en **Examinar**. Localice y seleccione una imagen para el icono del acceso directo. Los formatos de imagen compatibles son .png, .jpg, .jpeg.
6. Seleccione los tipos de dispositivo para los que desea configurar el acceso directo de la aplicación.
7. En cada una de las fichas de tipo de dispositivo que seleccionó, realice una de las siguientes acciones:
   - Agregue un acceso directo a un sitio web, en el campo URL, escriba la dirección web del acceso directo. La dirección web debe empezar por http:// o https://.
8. Seleccione la ubicación donde desea que aparezca el acceso directo que se va a añadir. Para dispositivos con BlackBerry Dynamics, especifique si desea que el acceso directo se abra en el navegador BlackBerry Access.
9. Haga clic en **Agregar**.

Tareas relacionadas

Asignación de una aplicación a un grupo de usuarios

Asignación de una aplicación a una cuenta de usuario

Cómo impedir que los usuarios instalen aplicaciones específicas.

Para ayudar a evitar que los usuarios instalen aplicaciones específicas, puede crear una lista de aplicaciones restringidas y utilizar perfiles de conformidad para imponer las restricciones. Por ejemplo, es posible que desee evitar que los usuarios instalen aplicaciones maliciosas o aplicaciones que requieran una gran cantidad de recursos.

Restringir aplicaciones específicas

Para dispositivos iOS, Android y Windows Phone, puede crear un perfil de conformidad para seleccionar aplicaciones de la lista de aplicaciones restringidas y establecer una acción de cumplimiento, como solicitar al usuario o eliminar datos de trabajo si se instala una de estas aplicaciones.

Para los siguientes dispositivos no es necesario especificar una acción de cumplimiento porque se impide automáticamente a los usuarios que instalen las aplicaciones especificadas en un perfil de conformidad:

- Para dispositivos con Windows Phone 8.1 y Samsung KNOX, si un usuario intenta instalar una aplicación restringida, el dispositivo mostrará un mensaje que indica que la aplicación está restringida y que no se puede instalar. Si la aplicación restringida ya está instalada, se desactiva. Para los dispositivos Samsung KNOX, puede seleccionar una opción en el perfil de conformidad para evitar que las aplicaciones se instalen en el espacio personal y en el espacio de trabajo.
- Para dispositivos supervisados con iOS 9.3.2 y posterior, si un usuario intenta instalar una aplicación restringida, la aplicación se oculta. Si una aplicación restringida ya está instalada, se oculta al usuario sin ninguna notificación. Para restringir las aplicaciones integradas, debe crear un perfil de conformidad y agregar las aplicaciones a la lista de aplicaciones restringidas del perfil. Para obtener más información, consulte iOS: configuración del perfil de conformidad.
- Para dispositivos con BlackBerry 10 y dispositivos Android que utilizan un perfil de trabajo, no tiene que crear un perfil de conformidad para restringir aplicaciones ya que los usuarios pueden instalar solo aplicaciones en el espacio de trabajo que usted haya asignado. Si la aplicación restringida ya está instalada en un dispositivo, no se desactiva.
- Para dispositivos Android que utilizan un perfil de trabajo, no tiene que crear un perfil de conformidad para restringir aplicaciones, que no sean aplicaciones del sistema, ya que los usuarios pueden instalar solo aplicaciones en el espacio de trabajo que usted haya asignado. Si la aplicación restringida ya está instalada en un dispositivo, no se desactiva. Si desea restringir una aplicación del sistema (como la calculadora, el reloj o la cámara), debe agregar la aplicación del sistema a un perfil de conformidad para forzar la restricción.

Permitir aplicaciones específicas

Para los dispositivos supervisados con iOS 9.3.2 y posterior, puede crear un perfil de conformidad que especifique una lista de aplicaciones permitidas. El resto de aplicaciones, con la excepción de las aplicaciones del teléfono y de preferencias, no están permitidas automáticamente y no se pueden ver en el dispositivo. Las aplicaciones que ya están instaladas y que no están en la lista de permitidos se ocultan al usuario sin ninguna notificación. Se incluyen las siguientes aplicaciones en la lista de permitidos de manera predeterminada para garantizar que los dispositivos se puedan gestionar en BlackBerry UEM:

- BlackBerry UEM Client
- Iconos de clips web
- BlackBerry Secure Connect Plus

Nota: Si se asigna la misma aplicación de iOS a la lista de restringidos y la lista de permitidos en un perfil de conformidad, la aplicación se restringirá.

Para obtener más información acerca de la creación de perfiles de conformidad, consulte Creación de un perfil de cumplimiento.

Pasos para impedir que los usuarios instalen aplicaciones específicas

Cuando impida que los usuarios instalen aplicaciones, debe realizar las acciones siguientes:

Paso	Acción
1	Agregue una aplicación a la lista de aplicaciones restringidas. **Nota:** Debe agregar aplicaciones a la lista de aplicaciones restringidas si desea restringir aplicaciones específicas o permitir aplicaciones específicas. **Nota:** Este paso no se aplica a las aplicaciones integradas para iOS 9.3.2 con supervisión y dispositivos posteriores. Para restringir las aplicaciones integradas, debe crear un perfil de conformidad y agregar las aplicaciones a la lista de aplicaciones restringidas del perfil. Para obtener más información, consulte iOS: configuración del perfil de conformidad.
2	Cree o edite un perfil de conformidad.
3	Asigne el perfil de cumplimiento a un usuario, a un grupo de usuarios o a un grupo de dispositivos.

Agregue una aplicación a la lista de aplicaciones restringidas

La lista de aplicaciones restringidas es una biblioteca de aplicaciones desde la que puede seleccionar si desea aplicar una de las siguientes reglas de conformidad:

- Aplicaciones restringidas instaladas (para dispositivos iOS, Android o Windows Phone).
- Mostrar solo las aplicaciones permitidas en el dispositivo (para dispositivos supervisados con iOS 9.3.2 y posterior)

1. En la barra de menú, haga clic en **Aplicaciones**.
2. Haga clic en **Aplicaciones restringidas**.
3. Haga clic en +.
4. Lleve a cabo una de las tareas siguientes:

Tarea	Pasos
Adición de una aplicación de iOS a la lista restringida	**a.** Haga clic en **Tienda de aplicaciones**. **b.** En el campo de búsqueda, busque la aplicación que desea agregar. Puede buscar por el nombre de la aplicación, el proveedor o la URL de App Store. **c.** Haga clic en **Buscar**. **d.** En los resultados de búsqueda, haga clic en **Agregar** para agregar una aplicación.

Tarea	Pasos
Adición de una aplicación de Android a la lista restringida	**a.** Haga clic en **Google Play**. **b.** En el campo **Nombre de aplicación**, escriba el nombre de la aplicación. **c.** En el campo **Dirección web de la aplicación de Google Play**, escriba la dirección web de la aplicación en Google Play. **d.** Haga clic en **Agregar** para agregar la aplicación o haga clic en **Agregar y crear nueva** para agregar otra aplicación después de agregar la aplicación actual.
Adición de una aplicación de Windows Phone a la lista restringida	**a.** Haga clic en **Tienda Windows**. **b.** En el campo **Nombre de aplicación**, escriba el nombre de la aplicación. **c.** En el campo **Dirección web de la aplicación de la Tienda Windows**, escriba la dirección web de la aplicación en la Windows Store. **d.** Haga clic en **Agregar** para agregar la aplicación o haga clic en **Agregar y crear nueva** para agregar otra aplicación después de agregar la aplicación actual.

Tareas relacionadas

Creación de un perfil de cumplimiento
Asignación de un perfil o una política de TI a un grupo de usuarios
Asignar un perfil o una política de TI a una cuenta de usuario
Creación de un grupo de dispositivos

Gestión de aplicaciones en la lista de aplicaciones

La lista de aplicaciones contiene las aplicaciones que se pueden asignar a los usuarios, a los grupos de usuarios y a los grupos de dispositivos. La lista de aplicaciones incluye la siguiente información:

- Icono y nombre de la aplicación
- Proveedor de la aplicación
- SO del dispositivo compatible
- Número de usuarios aplicados
- Número de dispositivos en los que la aplicación está instalada
- Clasificación de la aplicación
- Origen de la aplicación

Puede hacer clic en el número de usuarios aplicados para visualizar la información sobre el estado de la instalación de la aplicación.

Puede hacer clic en el número de dispositivos en los que está instalado la aplicación para ver un recuento de las instalaciones confirmadas y no confirmadas. Las instalaciones no confirmadas incluyen instalaciones en dispositivos iOS con el tipo de activación Privacidad del usuario porque UEM no puede confirmar si la aplicación sigue instalada en el dispositivo.

Las aplicaciones que aparecen con un icono de candado son aplicaciones de BlackBerry Dynamics. Para obtener más información, consulte Gestión de aplicaciones de BlackBerry Dynamics.

Nota: Las aplicaciones asignadas a los usuarios mediante un perfil de protección de aplicaciones de Microsoft Intune no aparecen en la lista de aplicaciones.

Eliminación de una aplicación de la lista de aplicaciones

Al eliminar una aplicación de la lista de aplicaciones, la aplicación queda sin asignar a los usuarios o grupos de usuarios a los que estuviera asignada y ya no aparece en el catálogo de aplicaciones de trabajo de un dispositivo.

1. En la barra de menús, haga clic en **Aplicaciones**.
2. Seleccione la casilla de verificación junto a las aplicaciones que desea eliminar de la lista de aplicaciones.
3. Haga clic en 🗑.
4. Haga clic en **Eliminar**.

Cambio de si una aplicación es obligatoria u opcional

Puede cambiar si una aplicación es obligatoria u opcional. Las acciones que se producen cuando una aplicación está establecida como obligatoria u opcional dependen del tipo de aplicación, del dispositivo y del tipo de activación.

1. En la barra de menús, haga clic en **Usuario y dispositivos**.
2. Si la aplicación que desea cambiar está asignada a una cuenta de usuario, en los resultados de la búsqueda, haga clic en el nombre de una cuenta de usuario.
3. Si la aplicación que desea cambiar está asignada a un grupo, en el panel izquierdo, haga clic en **Grupos** para ampliar la lista de grupos de usuarios y haga clic en el nombre del grupo.
4. En la sección **Aplicaciones asignadas a grupos y usuarios**, haga clic en la disposición de la aplicación que desea cambiar.
5. En la lista desplegable **Disposición** de la aplicación, seleccione **Opcional** u **Obligatorio**.
6. Haga clic en **Asignar**.

Referencia relacionada

Comportamiento de la aplicación en los dispositivos Android
Comportamiento de la aplicación en los dispositivos iOS
Comportamiento de la aplicación en los dispositivos BlackBerry

Notificaciones del dispositivo para aplicaciones nuevas y actualizadas

En la mayoría de los casos, los usuarios reciben notificaciones en sus dispositivos al asignar nuevas aplicaciones, o cuando hay actualizaciones disponibles para las aplicaciones instaladas. Además de las notificaciones de dispositivos, las aplicaciones nuevas o actualizadas aparecen en la lista "Nueva/Actualizada" del catálogo de aplicaciones en el BlackBerry UEM Client o en la aplicación Work Apps.

Las aplicaciones (obligatorias y opcionales) aparecen en la lista "Nueva/Actualizada" en las siguientes situaciones:

- Una aplicación se asigna a un usuario y la aplicación aún no está instalada en el dispositivo
- Una aplicación se asigna a un usuario y se instala automáticamente
- Está disponible una actualización para una aplicación instalada

BlackBerry UEM periódicamente reenviará notificaciones a los dispositivos si las aplicaciones permanecen en la lista "Nueva/Actualizada".

En la lista de aplicaciones "Nueva/actualizada", si un usuario hace clic en una nueva aplicación para ver los detalles, la aplicación se elimina de la lista "Nueva/actualizada", independientemente de si el usuario la instala.

Si un usuario hace clic en una aplicación actualizada, la aplicación permanece en la lista hasta que se instale la actualización.

Para obtener más información sobre notificaciones de aplicaciones, consulte:

- Comportamiento de la aplicación en los dispositivos iOS
- Comportamiento de la aplicación en los dispositivos Android
- Comportamiento de las aplicaciones en dispositivos Android que utilizan un perfil de trabajo
- Comportamiento de la aplicación en los dispositivos Samsung KNOX

Comportamiento de la aplicación en los dispositivos iOS

Para los dispositivos activados para BlackBerry Dynamics, el catálogo de aplicaciones de trabajo aparece en BlackBerry Dynamics Launcher si lo ha agregado a BlackBerry Dynamics Launcher.

Para dispositivos iOS activados con Controles de MDM y Privacidad del usuario, ocurre el comportamiento siguiente:

Tipo de aplicación	Cuando las aplicaciones están asignadas a un usuario	Cuando se actualizan las aplicaciones	Cuando las aplicaciones no están asignadas desde un usuario	Cuando se elimina el dispositivo de BlackBerry UEM
Aplicaciones públicas con una disposición obligatoria	Si ya se han instalado las aplicaciones, se le pregunta al usuario si desea permitirle a BlackBerry UEM gestionar las aplicaciones. En los dispositivos supervisados, las aplicaciones se instalan automáticamente. En los dispositivos no supervisados, no se pide a los usuarios que instalen las aplicaciones. Los usuarios deben acceder al catálogo de aplicaciones para instalar las aplicaciones necesarias. Las aplicaciones se quitan de la lista "Nuevas/ actualizaciones" cuando el usuario visualiza los detalles (incluso si la aplicación no está instalada), o cuando el usuario instala aplicaciones. Puede utilizar un perfil de cumplimiento para definir las acciones que se producen si no se instalan las aplicaciones obligatorias.	iTunes notifica a los usuarios de actualizaciones disponibles. Las aplicaciones se eliminarán de la lista "Nuevas/ actualizaciones" cuando el usuario actualice la aplicación. (puede tardar hasta una hora) Para los dispositivos que no tienen acceso a iTunes, no se notificará a los usuarios, pero podrán descargar la actualización del catálogo de aplicaciones.	Las aplicaciones se eliminan automáticamente del dispositivo sin notificación. Las aplicaciones ya no aparecen en el catálogo de aplicaciones.	Para los dispositivos activados con Controles de MDM, todas las aplicaciones se eliminan automáticamente. Para los dispositivos activados con Privacidad del usuario, se solicita a los usuarios que eliminen las aplicaciones.

Tipo de aplicación	Cuando las aplicaciones están asignadas a un usuario	Cuando se actualizan las aplicaciones	Cuando las aplicaciones no están asignadas desde un usuario	Cuando se elimina el dispositivo de BlackBerry UEM
Aplicaciones públicas con una disposición opcional	Si la aplicación ya está instalada, no ocurrirá nada. Se notifica al usuario cuando hay cambios en el catálogo de aplicaciones. Las aplicaciones se borran de la lista "nuevas/ actualizadas" solo cuando el usuario visualiza los detalles (independientemente de si la aplicación está instalada). Los usuarios pueden elegir si desean instalar las aplicaciones.	iTunes notifica a los usuarios de actualizaciones disponibles. Las aplicaciones se borran de la lista "nuevas/ actualizadas" cuando el usuario visualiza los detalles (independientemente de si la aplicación está actualizada).	Las aplicaciones se eliminan automáticamente del dispositivo. Las aplicaciones ya no aparecen en el catálogo de aplicaciones.	Para los dispositivos activados con Controles de MDM, todas las aplicaciones se eliminan automáticamente. Para los dispositivos activados con Privacidad del usuario, se solicita a los usuarios que eliminen las aplicaciones.

Tipo de aplicación	Cuando las aplicaciones están asignadas a un usuario	Cuando se actualizan las aplicaciones	Cuando las aplicaciones no están asignadas desde un usuario	Cuando se elimina el dispositivo de BlackBerry UEM
Aplicaciones internas con una disposición obligatoria	Si ya se han instalado las aplicaciones, se le pregunta al usuario si desea permitirle a BlackBerry UEM gestionar las aplicaciones. En los dispositivos supervisados, las aplicaciones se instalan automáticamente. En los dispositivos no supervisados, se pide a los usuarios que instalen las aplicaciones. Si el usuario cancela la instalación, puede instalar aplicaciones desde el catálogo de aplicaciones. Las aplicaciones se quitan de la lista "Nuevas/ actualizaciones" cuando el usuario visualiza los detalles (incluso si la aplicación no está instalada), o cuando el usuario instala aplicaciones. Puede utilizar un perfil de cumplimiento para definir las acciones que se producen si no se instalan las aplicaciones obligatorias.	Las aplicaciones se eliminarán de la lista "Nuevas/ actualizaciones" cuando el usuario actualice la aplicación.	Las aplicaciones se eliminan automáticamente del dispositivo sin notificación. Las aplicaciones ya no aparecen en el catálogo de aplicaciones.	Para los dispositivos activados con Controles de MDM, todas las aplicaciones se eliminan automáticamente. Para los dispositivos activados con Privacidad del usuario, se solicita a los usuarios que eliminen las aplicaciones.

Tipo de aplicación	Cuando las aplicaciones están asignadas a un usuario	Cuando se actualizan las aplicaciones	Cuando las aplicaciones no están asignadas desde un usuario	Cuando se elimina el dispositivo de BlackBerry UEM
Aplicaciones internas con una disposición opcional	Si las aplicaciones ya están instaladas, no ocurrirá nada. Las aplicaciones se quitan de la lista "Nuevas/ actualizaciones" cuando el usuario visualiza los detalles (incluso si la aplicación no está instalada), o cuando el usuario instala aplicaciones.	Las aplicaciones se eliminarán de la lista "Nuevas/ actualizaciones" cuando el usuario actualice la aplicación.	Las aplicaciones se eliminan automáticamente del dispositivo sin notificación. Las aplicaciones ya no aparecen en el catálogo de aplicaciones.	Para los dispositivos activados con Controles de MDM, todas las aplicaciones se eliminan automáticamente. Para los dispositivos activados con Privacidad del usuario, se solicita a los usuarios que eliminen las aplicaciones.

Comportamiento de la aplicación en los dispositivos Android

Para los dispositivos activados para BlackBerry Dynamics, el catálogo de aplicaciones de trabajo aparece en BlackBerry Dynamics Launcher si lo ha agregado a BlackBerry Dynamics Launcher.

Para dispositivos Android activados con Controles de MDM y Privacidad del usuario, ocurre el comportamiento siguiente:

Tipo de aplicación	Cuando las aplicaciones están asignadas a un usuario	Cuando se actualizan las aplicaciones	Cuando las aplicaciones no están asignadas desde un usuario	Cuando se elimina el dispositivo de BlackBerry UEM
Aplicaciones públicas con una disposición obligatoria	Se notifica al usuario cuando hay cambios en el catálogo de aplicaciones. Las aplicaciones se quitan de la lista "Nuevas/ actualizaciones" cuando el usuario visualiza los detalles (incluso si la aplicación no está instalada), o cuando el usuario instala aplicaciones. Puede utilizar un perfil de cumplimiento para definir las acciones que se producen si no se instalan las aplicaciones obligatorias.	Se envía una notificación al usuario mediante Google Play.	Al usuario se le indica que elimine las aplicaciones. Las aplicaciones ya no aparecen en el catálogo de aplicaciones.	Al usuario se le indica que elimine las aplicaciones.
Aplicaciones públicas con una disposición opcional	El usuario puede elegir si desea instalar las aplicaciones.	Se envía una notificación al usuario mediante Google Play.	Al usuario se le indica que elimine las aplicaciones. Las aplicaciones ya no aparecen en el catálogo de aplicaciones.	Al usuario se le indica que elimine las aplicaciones.

Tipo de aplicación	Cuando las aplicaciones están asignadas a un usuario	Cuando se actualizan las aplicaciones	Cuando las aplicaciones no están asignadas desde un usuario	Cuando se elimina el dispositivo de BlackBerry UEM
Aplicaciones internas con una disposición obligatoria	Se notifica al usuario cuando hay cambios en el catálogo de aplicaciones. Las aplicaciones se instalan automáticamente. Las aplicaciones se borran de la lista "Nuevas/ actualizadas" cuando el usuario visualiza los detalles o cuando la aplicación está instalada. Puede utilizar un perfil de cumplimiento para definir las acciones que se producen si no se instalan las aplicaciones obligatorias.	Se notifica al usuario cuando hay cambios en el catálogo de aplicaciones. Se han instalado las actualizaciones automáticamente. Las aplicaciones se borran de la lista "Nuevas/ actualizadas" cuando el usuario visualiza los detalles o cuando la aplicación está actualizada.	Al usuario se le indica que elimine las aplicaciones. Las aplicaciones ya no aparecen en el catálogo de aplicaciones.	Al usuario se le indica que elimine las aplicaciones.
Aplicaciones internas con una disposición opcional	El usuario puede elegir si desea instalar las aplicaciones. Las aplicaciones aparecen en la lista "Nuevas/ actualizadas".	Las aplicaciones aparecen en la lista "Nuevas/ actualizadas".	Al usuario se le indica que elimine las aplicaciones. Las aplicaciones ya no aparecen en el catálogo de aplicaciones.	Al usuario se le indica que elimine las aplicaciones.

Comportamiento de la aplicación en los dispositivos Samsung KNOX

Para los dispositivos activados para BlackBerry Dynamics, el catálogo de aplicaciones de trabajo aparece en BlackBerry Dynamics Launcher si lo ha agregado a BlackBerry Dynamics Launcher.

Para dispositivos Samsung KNOX activados con "Controles de MDM ", ocurre el comportamiento siguiente:

Tipo de aplicación	Cuando la aplicación está asignada a un usuario	Cuando se actualizan las aplicaciones	Cuando la aplicación no está asignada a un usuario	Cuando se elimina el dispositivo de BlackBerry UEM
Aplicaciones públicas con una disposición obligatoria	• Al usuario se le indica que instale las aplicaciones. • Las aplicaciones asignadas aparecen en BlackBerry UEM Client. Cuando el usuario hace clic en el botón Instalar, se abre Google Play y la aplicación se instala desde allí. • Puede utilizar un perfil de cumplimiento para definir las acciones que se producen si no se instalan las aplicaciones obligatorias.	• Google Play notifica a los usuarios de las actualizaciones. • La aplicación aparece en la lista "Nuevas/actualizadas".	• Al usuario se le indica que desinstale las aplicaciones.	• Al usuario se le indica que desinstale las aplicaciones de trabajo asignadas
Aplicaciones públicas con una disposición opcional	• El usuario puede elegir si desea instalar las aplicaciones. • Las aplicaciones asignadas aparecen en BlackBerry UEM Client. Cuando el usuario hace clic en el botón Instalar, se abre Google Play y las aplicaciones se instalan desde allí.	• Google Play notifica a los usuarios de las actualizaciones. • La aplicación aparece en la lista "Nuevas/actualizadas".	• Al usuario se le indica que desinstale las aplicaciones.	• Al usuario se le indica que desinstale las aplicaciones de trabajo asignadas

Tipo de aplicación	Cuando la aplicación está asignada a un usuario	Cuando se actualizan las aplicaciones	Cuando la aplicación no está asignada a un usuario	Cuando se elimina el dispositivo de BlackBerry UEM
Aplicaciones internas con una disposición obligatoria	• Las aplicaciones se instalan automáticamente en los dispositivos. El usuario no podrá desinstalar las aplicaciones.	• Las aplicaciones se actualizan automáticamente.	• Las aplicaciones se eliminan automáticamente del dispositivo.	• Las aplicaciones se eliminan automáticamente del dispositivo.
Aplicaciones internas con una disposición opcional	• El usuario puede elegir si desea instalar las aplicaciones. • El usuario instala aplicaciones desde BlackBerry UEM Client.	• El usuario puede elegir si desea actualizar las aplicaciones. • El usuario actualiza aplicaciones desde BlackBerry UEM Client.	• Las aplicaciones se eliminan automáticamente del dispositivo.	• Las aplicaciones se eliminan automáticamente del dispositivo.

Para los dispositivos activados que solo tienen espacio de trabajo (Samsung KNOX), ocurre el comportamiento siguiente:

Tipo de aplicación	Cuando la aplicación está asignada a un usuario	Cuando se actualizan las aplicaciones	Cuando la aplicación no está asignada a un usuario	Cuando se elimina el dispositivo de BlackBerry UEM
Aplicaciones públicas con una disposición obligatoria	• Todas las aplicaciones públicas se restringen de forma predeterminada en el espacio de trabajo. • Las aplicaciones asignadas aparecen en la lista "Nuevas/actualizadas", pero se deben instalar desde Google Play. • Las aplicaciones se borran de la lista "Nuevas/actualizadas" cuando el usuario visualiza los detalles o cuando la aplicación está actualizada. • Google Play debe estar activado en la política de TI que tiene asignada el usuario. • Puede utilizar un perfil de cumplimiento para definir las acciones que se producen si no se instala una aplicación obligatoria.	• Google Play notifica a los usuarios de las actualizaciones. • Las aplicaciones aparecen en la lista "Nuevas/actualizadas". • Las aplicaciones se borran de la lista "Nuevas/actualizadas" cuando el usuario visualiza los detalles o cuando la aplicación está actualizada.	• Las aplicaciones se eliminan del dispositivo y ya no se pueden instalar desde Google Play.	• El espacio de trabajo y todas las aplicaciones de trabajo se eliminan automáticamente. • Las aplicaciones ya no se restringen automáticamente en Google Play.

Tipo de aplicación	Cuando la aplicación está asignada a un usuario	Cuando se actualizan las aplicaciones	Cuando la aplicación no está asignada a un usuario	Cuando se elimina el dispositivo de BlackBerry UEM
Aplicaciones públicas con una disposición opcional	• Todas las aplicaciones públicas se restringen de forma predeterminada en el espacio de trabajo. • Las aplicaciones asignadas aparecen en la lista "Nuevas/actualizadas", pero se deben instalar desde Google Play. • Las aplicaciones se borran de la lista "Nuevas/actualizadas" cuando el usuario visualiza los detalles o cuando la aplicación está actualizada. • Google Play debe estar activado en la política de TI que tiene asignada el usuario.	• Google Play notifica a los usuarios de las actualizaciones. • Las aplicaciones aparecen en la lista "Nuevas/actualizadas". • Las aplicaciones se borran de la lista "Nuevas/actualizadas" cuando el usuario visualiza los detalles o cuando la aplicación está actualizada.	• Las aplicaciones se eliminan del dispositivo y ya no se pueden instalar desde Google Play.	• Las aplicaciones se eliminan automáticamente. • Las aplicaciones ya no se restringen automáticamente en Google Play.
Aplicaciones internas con una disposición obligatoria	• Las aplicaciones se instalan automáticamente en los dispositivos. El usuario no podrá desinstalar las aplicaciones.	• Las aplicaciones se actualizan automáticamente en el dispositivo.	• Las aplicaciones se eliminan automáticamente del dispositivo.	• Las aplicaciones se eliminan automáticamente del dispositivo.

Tipo de aplicación	Cuando la aplicación está asignada a un usuario	Cuando se actualizan las aplicaciones	Cuando la aplicación no está asignada a un usuario	Cuando se elimina el dispositivo de BlackBerry UEM
Aplicaciones internas con una disposición opcional	• Los usuarios pueden elegir si desean instalar las aplicaciones. • Los usuarios instalan aplicaciones desde BlackBerry UEM Client.	• Los usuarios pueden elegir si desean actualizar las aplicaciones. • Los usuarios actualizan aplicaciones desde BlackBerry UEM Client.	• Las aplicaciones se eliminan automáticamente del dispositivo.	• Las aplicaciones se eliminan automáticamente del dispositivo.

Para dispositivos activados con "Trabajo y personal: control total (Samsung KNOX)" y "Privacidad del usuario (Samsung KNOX)", ocurre el comportamiento siguiente:

Tipo de aplicación	Cuando la aplicación está asignada a un usuario	Cuando se actualizan las aplicaciones	Cuando la aplicación no está asignada a un usuario	Cuando se elimina el dispositivo de BlackBerry UEM
Aplicaciones públicas con una disposición obligatoria	• Todas las aplicaciones públicas se restringen de forma predeterminada en el espacio de trabajo. • Al usuario se le indica que instale las aplicaciones. • Las aplicaciones asignadas aparecen en BlackBerry UEM Client. Cuando el usuario hace clic en el botón Instalar, se abre Google Play y la aplicación se instala desde allí. • Puede utilizar un perfil de cumplimiento para definir las acciones que se producen si no se instalan las aplicaciones obligatorias.	• Google Play envía una notificación	• Las aplicaciones permanecen en el espacio personal pero se eliminan del espacio de trabajo.	• Se elimina el espacio de trabajo y las aplicaciones permanecen en el espacio personal.

Tipo de aplicación	Cuando la aplicación está asignada a un usuario	Cuando se actualizan las aplicaciones	Cuando la aplicación no está asignada a un usuario	Cuando se elimina el dispositivo de BlackBerry UEM
Aplicaciones públicas con una disposición opcional	• Todas las aplicaciones se restringen de forma predeterminada en el espacio de trabajo. • Las aplicaciones asignadas aparecen en BlackBerry UEM Client, pero se deben instalar desde Google Play. • Google Play debe estar activado en la política de TI que tiene asignada el usuario.	• Google Play envía una notificación	• Las aplicaciones permanecen en el espacio personal pero se eliminan del espacio de trabajo.	• Se elimina el espacio de trabajo y las aplicaciones permanecen en el espacio personal.
Aplicaciones internas con una disposición obligatoria	• Las aplicaciones se instalan automáticamente en el espacio de trabajo. El usuario no podrá desinstalar las aplicaciones.	• Las actualizaciones se instalan automáticamente.	• Las aplicaciones se eliminan automáticamente del dispositivo.	• Se elimina el espacio de trabajo y las aplicaciones permanecen en el espacio personal.
Aplicaciones internas con una disposición opcional	• Los usuarios pueden elegir si desean instalar las aplicaciones. • El usuario instala aplicaciones desde BlackBerry UEM Client y se instalan en el espacio de trabajo.	• Los usuarios pueden elegir si desean actualizar las aplicaciones. • Los usuarios actualizan aplicaciones desde BlackBerry UEM Client.	• Las aplicaciones se eliminan automáticamente del dispositivo.	• Se elimina el espacio de trabajo y las aplicaciones permanecen en el espacio personal.

Comportamiento de las aplicaciones en dispositivos Android que utilizan un perfil de trabajo

Para los dispositivos activados para BlackBerry Dynamics, el catálogo de aplicaciones de trabajo aparece en BlackBerry Dynamics Launcher si lo ha agregado a BlackBerry Dynamics Launcher.

Para dispositivos activados con "Trabajo y personal: privacidad de usuario " o "Solo espacio de trabajo " ocurre el comportamiento siguiente:

Tipo de aplicación	Cuando la aplicación está asignada a un usuario	Cuando se actualizan las aplicaciones	Cuando la aplicación no está asignada a un usuario	Cuando se elimina el dispositivo de BlackBerry UEM
Aplicaciones públicas con una disposición obligatoria	• Las aplicaciones se instalan automáticamente.	• Las aplicaciones se actualizan automáticamente.	• Las aplicaciones se eliminan automáticamente del dispositivo.	• El perfil de trabajo y las aplicaciones de trabajo asignadas se eliminan del dispositivo.
Aplicaciones públicas con una disposición opcional	• El usuario puede elegir si desea instalar las aplicaciones. • Las aplicaciones aparecen en Google Play for Work.	• Google Play for Work notifica a los usuarios acerca de las actualizaciones.	• Las aplicaciones se eliminan automáticamente del dispositivo.	• El perfil de trabajo y las aplicaciones de trabajo asignadas se eliminan del dispositivo.
Aplicaciones internas con una disposición obligatoria alojadas en BlackBerry UEM	• No es compatible. Solo son compatibles las aplicaciones internas con una disposición opcional.	• No es compatible. Solo son compatibles las aplicaciones internas con una disposición opcional.	• No es compatible. Solo son compatibles las aplicaciones internas con una disposición opcional.	• No es compatible. Solo son compatibles las aplicaciones internas con una disposición opcional.
Aplicaciones internas con una disposición opcional alojadas en BlackBerry UEM	• El usuario puede elegir si desea instalar las aplicaciones. • Las aplicaciones aparecen en Google Play for Work.	• Google Play for Work notifica a los usuarios acerca de las actualizaciones.	• Las aplicaciones se eliminan automáticamente del dispositivo.	• El perfil de trabajo y las aplicaciones de trabajo asignadas se eliminan del dispositivo.

Tipo de aplicación	Cuando la aplicación está asignada a un usuario	Cuando se actualizan las aplicaciones	Cuando la aplicación no está asignada a un usuario	Cuando se elimina el dispositivo de BlackBerry UEM
Aplicaciones internas con una disposición obligatoria alojadas en Google Play	• Las aplicaciones se instalan automáticamente en el dispositivo.	• Google Play for Work notifica a los usuarios acerca de las actualizaciones.	• Las aplicaciones se eliminan automáticamente del dispositivo.	• El perfil de trabajo y las aplicaciones de trabajo asignadas se eliminan del dispositivo.
Aplicaciones internas con una disposición opcional alojadas en Google Play	• El usuario puede elegir si desea instalar las aplicaciones. • Las aplicaciones aparecen en Google Play for Work.	• Google Play for Work notifica a los usuarios acerca de las actualizaciones.	• Las aplicaciones se eliminan automáticamente del dispositivo.	• El perfil de trabajo y las aplicaciones de trabajo asignadas se eliminan del dispositivo.

Comportamiento de la aplicación en los dispositivos BlackBerry

Para dispositivos BlackBerry activados con Trabajo y personal - Empresa (Solo espacio de trabajo) o Trabajo y personal - Regulado, ocurre lo siguiente:

Tipo de aplicación	Comportamiento cuando las aplicaciones están asignadas a un usuario	Comportamiento cuando las aplicaciones no están asignadas a un usuario	Comportamiento cuando se elimina el dispositivo de BlackBerry UEM
Aplicaciones públicas con una disposición obligatoria	No es compatible.	No es compatible.	No es compatible.
Aplicaciones públicas con una disposición opcional	El usuario puede elegir si desea instalar las aplicaciones. Las aplicaciones aparecen en la pestaña Aplicaciones públicas en BlackBerry World para el trabajo.	Al usuario se le indica que desinstale las aplicaciones.	El espacio de trabajo y todas las aplicaciones de trabajo se eliminan automáticamente.

Tipo de aplicación	Comportamiento cuando las aplicaciones están asignadas a un usuario	Comportamiento cuando las aplicaciones no están asignadas a un usuario	Comportamiento cuando se elimina el dispositivo de BlackBerry UEM
Aplicaciones internas con una disposición obligatoria	Las aplicaciones se instalan automáticamente en los dispositivos. El usuario no podrá desinstalar las aplicaciones.	Las aplicaciones se eliminan automáticamente del dispositivo.	El espacio de trabajo y todas las aplicaciones de trabajo se eliminan automáticamente.
Aplicaciones internas con una disposición opcional	Las aplicaciones se instalan automáticamente en los dispositivos. El usuario no podrá desinstalar las aplicaciones.	Las aplicaciones se eliminan automáticamente del dispositivo.	El espacio de trabajo y todas las aplicaciones de trabajo se eliminan automáticamente.

Comportamiento de la aplicación en los dispositivos Windows 10

Tipo de aplicación	Comportamiento cuando las aplicaciones están asignadas a un usuario	Comportamiento cuando las aplicaciones no están asignadas a un usuario	Comportamiento cuando los dispositivos se eliminan de BlackBerry UEM
Aplicaciones de Windows Store sin conexión con una disposición obligatoria	• Las aplicaciones se instalan automáticamente en los dispositivos. Los usuarios no podrán desinstalar las aplicaciones.	• Las aplicaciones se eliminan automáticamente de los dispositivos.	• Las aplicaciones se eliminan automáticamente de los dispositivos.
Aplicaciones de Windows Store en línea con una disposición obligatoria	• Las aplicaciones se instalan automáticamente en los dispositivos. Los usuarios no podrán desinstalar las aplicaciones.	• Las aplicaciones se eliminan automáticamente de los dispositivos.	• Las aplicaciones se eliminan automáticamente de los dispositivos.

Tipo de aplicación	Comportamiento cuando las aplicaciones están asignadas a un usuario	Comportamiento cuando las aplicaciones no están asignadas a un usuario	Comportamiento cuando los dispositivos se eliminan de BlackBerry UEM
Aplicaciones de Windows Store sin conexión con una disposición opcional	• Los usuarios pueden elegir si desean instalar las aplicaciones. • Para las aplicaciones sin conexión, los usuarios instalan la aplicación desde BlackBerry UEM App Catalog. • No compatibles con los dispositivos Windows 10 Mobile.	• A los usuarios no se les indica que desinstalen las aplicaciones.	• A los usuarios no se les indica que desinstalen las aplicaciones asignadas.
Aplicaciones Windows Store en línea con una disposición opcional	• Los usuarios pueden elegir si desean instalar las aplicaciones. • Para las aplicaciones en línea, los usuarios instalan la aplicación desde la aplicación Windows Store de sus dispositivos. • No compatibles con los dispositivos Windows 10 Mobile.	• A los usuarios no se les indica que desinstalen las aplicaciones.	• A los usuarios no se les indica que desinstalen las aplicaciones.
Aplicaciones internas con una disposición obligatoria	• No es compatible	• No es compatible	• No es compatible
Aplicaciones internas con una disposición opcional	• No es compatible	• No es compatible	• No es compatible

Administración de grupos de aplicaciones

Los grupos de aplicaciones permiten crear una recopilación de aplicaciones que se pueden asignar a los usuarios, a los grupos de usuarios o a los grupos de dispositivos. La agrupación de aplicaciones ayuda a aumentar la eficiencia y la coherencia al administrar aplicaciones. Por ejemplo, puede utilizar grupos de aplicaciones para agrupar las mismas aplicaciones para varios tipos de dispositivos o para agrupar aplicaciones para usuarios con la misma función en la empresa.

BlackBerry UEM proporciona un grupo de aplicaciones preconfiguradas denominado "Aplicaciones recomendadas para dispositivos Android con un perfil de trabajo" y "BlackBerry Productivity Suite".

Creación de un grupo de aplicaciones

Antes de empezar: Agregue las aplicaciones a la lista de aplicaciones.

1. En la barra de menús, haga clic en **Aplicaciones > Grupos de aplicaciones**.
2. Haga clic en .
3. Escriba un nombre y una descripción para el grupo de aplicaciones.
4. Haga clic en .
5. Busque y seleccione las aplicaciones que desee agregar.
6. Para aplicaciones de iOS y Android, si hay disponible una configuración de aplicaciones, seleccione la configuración de aplicaciones que desee asignar a la aplicación.
7. Si agrega aplicaciones de iOS, realice una de las tareas siguientes:

Tarea	Pasos
Si no ha agregado una cuenta de VPP	**a.** Haga clic en **Agregar**.
Si al menos ha agregado una cuenta de VPP	**a.** Haga clic en **Agregar**. **b.** Seleccione **Sí** si desea asignar una licencia a la aplicación de iOS. Seleccione **No** si no desea asignar una licencia o no tiene una licencia que asignar a la aplicación. **c.** Si asigna una licencia a la aplicación, en la lista desplegable **Licencia de la aplicación**, seleccione la cuenta de VPP para asociarla a la aplicación. **d.** En la lista desplegable **Asignar licencia a**, asigne la licencia al **Usuario** o al **Dispositivo**. Si la lista desplegable **Licencia de la aplicación** no está especificada, la lista desplegable **Asignar licencia a** no está disponible. **e.** Haga clic en **Agregar** y, a continuación, haga clic en **Agregar** de nuevo. Los usuarios deben seguir las instrucciones en sus dispositivos para inscribirse en el programa de compras por volumen (VPP) de la empresa antes de poder instalar aplicaciones de prepago. Los usuarios deben completar esta tarea una vez. **Nota:** Si concede acceso a un número de licencias superior al número de licencias disponibles, los primeros usuarios que accedan a las licencias disponibles podrán instalar la aplicación.

8. Haga clic en **Agregar** y, a continuación, haga clic en **Agregar** de nuevo.

Tareas relacionadas

Asignación de una aplicación a un grupo de usuarios
Asignación de una aplicación a una cuenta de usuario

Edición de un grupo de aplicaciones

1. En la barra de menús, haga clic en **Aplicaciones > Grupos de aplicaciones**.

2. Haga clic en el grupo de aplicaciones que desea editar.
3. Realice las ediciones necesarias.
4. Haga clic en **Guardar**.

Presentación del estado de las aplicaciones y los grupos de aplicaciones asignados a las cuentas de usuario

1. En la barra de menús, haga clic en **Aplicaciones**.
2. En la opción **Usuarios aplicados** correspondiente a la aplicación o el grupo de aplicaciones que desea ver, haga clic en el número.
3. Haga clic en **Asignación para *x* usuarios** para ver las cuentas de usuarios a la que está asignada esta aplicación
4. Consulte la columna **Asignación** para verificar si la aplicación o el grupo de aplicaciones se han asignado directamente a la cuenta de usuario o a un grupo.
5. Consulte la columna **Estado** para verificar si se ha instalado una aplicación en un dispositivo. Los posibles estados son los siguientes:
   - **Instalada**: la aplicación se ha instalado en el dispositivo del usuario. Para los dispositivos iOS con el tipo de activación Privacidad del usuario, este estado indica que solo se ha iniciado la instalación. BlackBerry UEM no puede confirmar si la aplicación sigue instalada en el dispositivo.
   - **No instalada**: la aplicación no se ha instalado en el dispositivo del usuario o se ha eliminado del dispositivo del usuario.
   - **No puede instalarse**: la aplicación no es compatible con el dispositivo del usuario.
   - **No es compatible**: el sistema operativo del dispositivo no es compatible con la aplicación.

Presentación de las aplicaciones que están asignadas a grupos de usuarios

1. En la barra de menús, haga clic en **Aplicaciones**.
2. En **Asignación para usuarios** correspondiente a la aplicación que desea ver, haga clic en el número.
3. Haga clic en **Asignado a *x* grupos** para ver los grupos de usuarios a los que está asignada esta aplicación.

Presentación y personalización de la lista de aplicaciones

Puede personalizar la lista de aplicaciones y seleccionar la información que desee visualizar. Puede utilizar filtros para ver únicamente la información relevante para su tarea. Puede seleccionar y reordenar las columnas de la lista de aplicaciones. Puede agregar y eliminar columnas en la lista de aplicaciones. Puede utilizar uno o varios filtros para controlar las aplicaciones que se muestran. Por ejemplo, puede filtrar la lista de aplicaciones por tipo de aplicación, sistema operativo, categoría, tipo protegido y valoración de la aplicación.

Seleccione la información que desea que aparezca en la lista de aplicaciones

1. En la barra de menú, haga clic en **Aplicaciones > Todas las aplicaciones**.
2. Haga clic en + en la parte superior de la lista de aplicaciones y realice cualquiera de las siguientes acciones:
   - Haga clic en **Seleccionar todo** o seleccione la casilla de verificación correspondiente a cada columna que desee mostrar.
   - Desactive la casilla de verificación correspondiente a cada una de las columnas que desea eliminar.
   - Haga clic en **Restablecer** para volver a las selecciones predeterminadas.
3. Para volver a ordenar las columnas, haga clic en el encabezado de una columna y arrástrelo hacia la izquierda o la derecha.

Filtrado de la lista de aplicaciones

Al activar la selección múltiple, puede seleccionar varios filtros antes de aplicarlos y también seleccionar varios filtros en cada categoría. Si desactiva la selección múltiple, cada filtro se aplicará cuando lo seleccione y solo puede seleccionar un filtro en cada categoría.

1. En la barra de menús, haga clic en **Aplicaciones > Todas las aplicaciones**.
2. Haga clic en para activar o desactivar la selección múltiple.
3. En **Filtros**, amplíe una o más categorías.

   Cada categoría incluye solo los filtros que muestran resultados y cada filtro indica el número de resultados que se mostrarán al aplicarlo.
4. Lleve a cabo una de las siguientes acciones:
   - Si activó la selección múltiple, seleccione la casilla de verificación de cada filtro que desea aplicar y haga clic en **Enviar**.
   - Si desactivó la selección múltiple, haga clic en el filtro que desea aplicar.
5. De manera opcional, en el panel derecho, haga clic en **Borrar todo** o haga clic en para cada filtro que desee eliminar.

Actualización de la lista de aplicaciones

Puede actualizar la lista de aplicaciones para asegurarse de tener la información más reciente acerca de las aplicaciones deBlackBerry 10,iOS,Windows 10yBlackBerry Dynamicsen la lista de aplicaciones.

Si tiene BlackBerry UEM configurado para que sea compatible con perfiles de trabajo de Android, también puede actualizar la información de la aplicación para las aplicaciones de Android. Si ha agregado aplicaciones de Android antes de haber configurado la compatibilidad para perfiles de trabajo de Android o de que los permisos de aplicaciones hayan cambiado, debe actualizar la información de la aplicación para ponerlos a disposición de los dispositivos Android con un perfil de trabajo. Esto también se aplica si realiza cambios en la configuración del perfil de trabajo de Android.

Si no ha configurado la compatibilidad para perfiles de trabajo de Android o aplicaciones de Windows Phone, la información acerca de las aplicaciones de Google Play debe actualizarse manualmente. La actualización de la información de la aplicación no significa que la aplicación se actualice en el dispositivo del usuario. Los usuarios reciben notificaciones de actualización para sus aplicaciones de trabajo del mismo modo que reciben notificaciones de actualización para sus aplicaciones personales.

Si ha configurado su cuenta de VPP de Apple para actualizar automáticamente la información de la aplicación para las aplicaciones de iOS, debe actualizar las aplicaciones de la lista de aplicaciones.

1. En la barra de menús, haga clic en **Aplicaciones**.
2. Haga clic en.

Actualizar permisos de aplicaciones para aplicaciones con perfiles de trabajo de Android

Si no acepta los permisos de aplicaciones en nombre de los usuarios, las aplicaciones no se pueden asignar a dispositivos Android con un perfil de trabajo. Se deben aceptar los permisos de aplicaciones cuando agregue la aplicación a la lista de aplicaciones y se podría tener que volver a aceptar posteriormente si los permisos de aplicaciones cambian.

Las aplicaciones también pueden no aprobarse o eliminarse desde la consola de Google Play pero seguir apareciendo como si estuvieran disponibles en BlackBerry UEM. Debe actualizar la información de la aplicación en BlackBerry UEM para sincronizar los permisos con Google Play.

1. En la barra de menú, haga clic en **Aplicaciones**.

2. Haga clic en .
3. En la lista de aplicaciones, las aplicaciones con cambios de permiso se muestran con un icono de advertencia y un mensaje de estado. Los estados siguientes pueden darse después de actualizar la lista de aplicaciones. Realice una de las siguientes tareas para solucionar el problema:

Estado	Pasos
Reaceptar permisos de aplicación	Los permisos de la aplicación se han cambiado en la consola de Google Play. Para poder administrar la aplicación, se deben volver a aceptar los permisos de la aplicación. Para volver a aceptar permisos, complete los siguientes pasos: **a.** Haga clic en **Reaceptar permisos de aplicación**. **b.** Haga clic en **Aceptar**.
Eliminar aplicación de BlackBerry UEM	La aplicación no se aprobó desde la consola de Google Play pero no se eliminó de BlackBerry UEM. Si desea continuar gestionando la aplicación en los dispositivos, debe aprobar la aplicación en la consola de Google Play. Si ya no desea administrar la aplicación, realice los siguientes pasos: **a.** Haga clic en **Eliminar aplicación de BlackBerry UEM**. **b.** Haga clic en **Eliminar**.
Apruebe la aplicación en Google Play	La aplicación no se aprobó en la consola de Google Play. Para poder administrar la aplicación, se deben aprobar los permisos en la consola de Google Play. Para aprobar la aplicación, complete los siguientes pasos: **a.** Haga clic en **Aprobar aplicación en Google Play**. **b.** Acepte los permisos de la aplicación. **c.** Haga clic en **Aceptar**.
Se agregó la aplicación en Google Play y se va a agregar a BlackBerry UEM	Las aplicaciones que se han agregado a la consola de Google Play for Work, pero no a BlackBerry UEM, se sincronizan automáticamente con BlackBerry UEM cuando se actualiza la lista de aplicaciones. No se tiene que realizar ninguna acción.

4. Haga clic en **Cerrar**.

Aceptar permisos de aplicaciones para aplicaciones con perfiles de trabajo de Android

Debe aceptar los permisos de aplicaciones antes de que pueda gestionar las aplicaciones en dispositivos Android con un perfil de trabajo. Puede aceptar los permisos de aplicaciones cuando agregue la aplicación a BlackBerry UEM o después de actualizar la lista de aplicaciones. Si no acepta los permisos de aplicaciones en estos casos, también puede aceptar los permisos de aplicaciones desde la pantalla de información de la aplicación. Las aplicaciones que tienen cambios de permisos se muestran con un icono de advertencia en la lista aplicaciones.

Antes de empezar:

- Actualice la lista de aplicaciones.

1. En la barra de menús, haga clic en **Aplicaciones**.
2. Haga clic en la aplicación para la que desea aceptar los permisos.
3. Haga clic en **Aceptar permisos de aplicación** para aceptar los permisos de aplicaciones.

4. Seleccione **Aceptar**.
5. Haga clic en **Guardar**.

Gestión de aplicaciones de BlackBerry Dynamics

Si su empresa utiliza aplicaciones de BlackBerry Dynamics, puede que deba configurar ajustes de aplicaciones adicionales. Por ejemplo, si su empresa utiliza BlackBerry Work, configure los ajustes de la aplicación para enviar correo a los dispositivos en lugar de utilizar un perfil de correo. También debe configurar los ajustes de conectividad y otras opciones que se aplican solo a aplicaciones de BlackBerry Dynamics.

Para obtener más información sobre las funciones y configuraciones que admiten las aplicaciones de BlackBerry Dynamics individuales, consulte los recursos para administradores de la aplicación.

Para utilizar las aplicaciones de BlackBerry Dynamics en su empresa, debe realizar las acciones siguientes:

Paso	Acción
1	Compruebe la configuración de conectividad de BlackBerry Dynamics y cámbiela si es necesario.
2	Cree un perfil de BlackBerry Dynamics o actualice el perfil de BlackBerry Dynamics predeterminado.
3	Agregue aplicaciones de BlackBerry Dynamics a BlackBerry UEM.
4	Si es necesario, cambie la configuración de las aplicaciones de BlackBerry Dynamics.
5	Adición del catálogo de aplicaciones de trabajo a BlackBerry Dynamics Launcher.
6	Asigne el perfil de BlackBerry Dynamics y el perfil de conectividad de BlackBerry Dynamics a un grupo de usuarios o una cuenta de usuario.
7	Asigne aplicaciones de BlackBerry Dynamics a grupos de usuarios o cuentas de usuario.
8	Para los usuarios que desean activar aplicaciones de UEM Client en dispositivos sin BlackBerry Dynamics, genere claves de acceso para las aplicaciones.

Gestión de la configuración de una aplicación de BlackBerry Dynamics

Puede gestionar configuraciones de aplicaciones, configuraciones de servidores y opciones de aplicaciones.

1. En la barra de menú, haga clic en **Aplicaciones**.
2. Haga clic en la aplicación de BlackBerry Dynamics que desea cambiar.
3. En la pestaña **Configuración > BlackBerry Dynamics**, realice cualquiera de las siguientes tareas:

Tarea	Pasos
Especificar un perfil de BlackBerry Dynamics para la aplicación.	Si desea que la aplicación utilice un perfil de BlackBerry Dynamics específico en lugar del perfil de BlackBerry Dynamics que se ha asignado al usuario, seleccione el perfil de la lista desplegable de perfiles **Anular BlackBerry Dynamics**.
Especificar un perfil de conformidad para la aplicación.	Si desea que la aplicación utilice un perfil de conformidad específico en lugar del perfil de conformidad que se ha asignado al usuario, seleccione el perfil de la lista desplegable de perfiles **Anular perfil de conformidad**.
Agregar o cambiar la configuración de la aplicación para una aplicación interna.	**a.** Junto a **Configuración de la aplicación**, haga clic en **Cargar una plantilla** para agregar una nueva plantilla de configuración de la aplicación. **b.** Busque la ubicación de la plantilla. **c.** Haga clic en **Guardar**.
Agregar o cambiar la configuración de la aplicación para una aplicación pública	**a.** En la sección **Configuración de AirPrint**, haga clic en +. **b.** Escriba un nombre para la configuración de la aplicación. **c.** Edite la configuración. **d.** Haga clic en **Guardar**. **e.** Si es necesario, utilice las flechas para mover la configuración de la aplicación hacia arriba o hacia abajo para cambiar la prioridad. Para obtener más información, consulte Opciones de configuración de la aplicación BlackBerry UEM Client. Para obtener más información acerca de la configuración de los ajustes de las aplicaciones BlackBerry Work, BlackBerry Notes y BlackBerry Tasks, consulte Configurar los ajustes de la aplicación BlackBerry Work y Configurar los ajustes de las aplicaciones BlackBerry Notes y BlackBerry Tasks en el contenido Administración de BlackBerry Work, Notes y Tasks.
Agregue o cambie la carga de configuración del servidor para especificar las claves y valores que se utilizan para configurar las opciones de la aplicación.	Si la aplicación tiene políticas de aplicaciones personalizadas, las políticas personalizadas se agregan al área de carga de configuración del servidor. **a.** En la sección **Carga de configuración del servidor**, haga clic en **Agregar**. **b.** En el cuadro de texto, introduzca el código XML o JSON para la carga de configuración.
Permitir que las aplicaciones de BlackBerry Dynamics utilicen certificados de usuario, perfiles SCEP y perfiles de credenciales de usuario	Seleccione si la aplicación puede utilizar certificados de usuario como una opción de autenticación. Para obtener más información sobre la configuración del entorno para utilizar certificados con aplicaciones de BlackBerry Dynamics, consulte Envío de certificados a dispositivos mediante perfiles.

4. Haga clic en la pestaña de la plataforma del dispositivo que desea gestionar y ajuste las opciones correspondientes.
5. Haga clic en **Guardar**.

iOS y macOS: configuración de la aplicación BlackBerry Dynamics

La mayoría de las configuraciones siguientes son compatibles únicamente con dispositivos iOS y no aparecen en la pestaña macOS.

iOS Configuración de y macOS	Descripción
ID de paquete de aplicación iOS o macOS	En la configuración se especifica el ID de paquete de la aplicación.
Nombre de la aplicación	Esta configuración especifica el nombre de la aplicación que aparece en la lista de aplicaciones.
Proveedor	Esta configuración especifica el proveedor de la aplicación.
Descripción de la aplicación	Esta configuración especifica la descripción de la aplicación.
Categoría	Esta configuración especifica una categoría para filtrar aplicaciones en la lista de aplicaciones por categoría y para organizar las aplicaciones en categorías en la lista de aplicaciones de trabajo en los dispositivos de los usuarios. Puede seleccionar una categoría o escribir un nombre para crear una categoría nueva.
Capturas de pantalla	Esta configuración especifica las capturas de pantalla de la aplicación. Haga clic en "Agregar" para seleccionar las imágenes. Los tipos de imagen compatibles son .jpg, .jpeg, .png, o .gif.
Factor de forma compatible del dispositivo	Esta configuración especifica los factores de forma en los que se puede instalar la aplicación. Por ejemplo, puede evitar que la aplicación esté disponible en la aplicación Work Apps en iPad.
Eliminar la aplicación del dispositivo cuando este se haya eliminado de BlackBerry UEM	Esta configuración especifica si la aplicación se elimina del dispositivo cuando este se elimina de BlackBerry UEM. Esta configuración se aplica únicamente cuando la disposición de la aplicación se establece como "Obligatoria" y la opción de instalación predeterminada para las aplicaciones obligatorias se establece en "Preguntas una vez".
Desactivar copia de seguridad en iCloud para la aplicación	En la configuración se especifica si se puede realizar una copia de seguridad de la aplicación en el servicio en línea iCloud. Esta opción se aplica únicamente cuando la disposición de la aplicación se establece como "Obligatoria".

iOS Configuración de y macOS	Descripción
Instalación predeterminada para las aplicaciones obligatorias	Esta configuración especifica si se solicita a los usuarios que instalen aplicaciones obligatorias. Seleccione una de las siguientes opciones: • **Preguntar una vez**: los usuarios reciben una solicitud para instalar la aplicación en sus dispositivos iOS. Si los usuarios descartan la solicitud, pueden instalar la aplicación más adelante mediante la pantalla Work Apps en la aplicación BlackBerry UEM Client o en el icono Work Apps del dispositivo. • **No preguntar**: los usuarios no reciben una solicitud para instalar la aplicación. Esta configuración se aplica únicamente a aplicaciones con la disposición establecida en "Obligatoria". La disposición de la aplicación se establece al asignarse a un usuario o grupo.
Convertir aplicación personal instalada en aplicación de trabajo	Esta configuración especifica si se convierte la aplicación en una aplicación de trabajo si ya está instalada en los dispositivos con iOS 9 o posterior. Si selecciona "Convertir", después de asignar la aplicación a un usuario, la aplicación se convierte en una aplicación de trabajo y se puede gestionar con BlackBerry UEM.
Versiones restringidas	Esta configuración especifica las versiones de la aplicación que desea impedir que los usuarios instalen en sus dispositivos. Si agrega varias versiones, separe cada versión con una coma.

Android: configuración de la aplicación BlackBerry Dynamics

Configuración de Android	Descripción
ID de paquete de aplicación Android	En la configuración se especifica el ID de paquete de la aplicación.
Nombre de la aplicación	Esta configuración especifica el nombre de la aplicación que aparece en la lista de aplicaciones.
Proveedor	Esta configuración especifica el proveedor de la aplicación.
Descripción de la aplicación	Esta configuración especifica la descripción de la aplicación.
Categoría	Esta configuración especifica una categoría para filtrar aplicaciones en la lista de aplicaciones por categoría y para organizar las aplicaciones en categorías en la lista de aplicaciones de trabajo en los dispositivos de los usuarios. Puede seleccionar una categoría o escribir un nombre para crear una categoría nueva.
Enviar a	Esta configuración especifica si la aplicación se envía a todos los dispositivos Android, solo a los dispositivos Android con un perfil de trabajo o solo a los dispositivos Samsung KNOX Workspace.

Configuración de Android	Descripción
Versiones restringidas	Esta configuración especifica las versiones de la aplicación que desea impedir que los usuarios instalen en sus dispositivos. Si agrega varias versiones, separe cada versión con una coma.

Windows: configuración de la aplicación BlackBerry Dynamics

Configuración de Windows	Descripción
ID de paquete de aplicaciones de Windows Phone 8.1	Esta configuración especifica el ID de paquete de una aplicación Windows Phone 8.1.
Nombre de la familia del paquete de Windows 10 (UWP)	Esta configuración especifica el nombre de la familia del paquete de una aplicación Windows 10.
Nombre de la aplicación	Esta configuración especifica el nombre de la aplicación que aparece en la lista de aplicaciones.
Proveedor	Esta configuración especifica el proveedor de la aplicación.
Descripción de la aplicación	Esta configuración especifica la descripción de la aplicación.
Categoría	Esta configuración especifica una categoría para filtrar aplicaciones en la lista de aplicaciones por categoría y para organizar las aplicaciones en categorías en la lista de aplicaciones de trabajo en los dispositivos de los usuarios. Puede seleccionar una categoría o escribir un nombre para crear una categoría nueva.
Capturas de pantalla	Esta configuración especifica las capturas de pantalla de la aplicación. Haga clic en "Agregar" para seleccionar las imágenes. Los tipos de imagen compatibles son .jpg, .jpeg, .png, o .gif.
Eliminar la aplicación del dispositivo cuando este se haya eliminado de BlackBerry UEM	Esta configuración especifica si la aplicación se elimina del dispositivo cuando este se elimina de BlackBerry UEM. Esta configuración se aplica únicamente cuando la disposición de la aplicación se establece como "Obligatoria" y la opción de instalación predeterminada para las aplicaciones obligatorias se establece en "Preguntas una vez".
Versiones restringidas	Esta configuración especifica las versiones de la aplicación que desea impedir que los usuarios instalen en sus dispositivos. Si agrega varias versiones, separe cada versión con una coma.

Opciones de configuración de la aplicación BlackBerry UEM Client

Opción	Descripción
Permitir el uso de Bypass Unlock en UEM Client	Si selecciona esta opción, UEM Client desviará la pantalla de bloqueo/autenticación de usuario de BlackBerry Dynamics y el usuario podrá abrir UEM Client sin necesidad de desbloquear la aplicación UEM Client. Si ha configurado BlackBerry 2FA, se mostrará la pantalla de aceptación/rechazo de BlackBerry 2FA y el usuario deberá hacer clic en Aceptar. A continuación, el usuario debe iniciar sesión en la aplicación o el servicio a través de BlackBerry 2FA.
Nombre de la aplicación	Escriba un nombre para la aplicación. Seleccione esta opción si desea utilizar la solución PKI basada en aplicación de su empresa, como Purebred, para inscribir certificados para aplicaciones de BlackBerry Dynamics. Puede instalar la aplicación en dispositivos y permitir que las aplicaciones de BlackBerry Dynamics utilicen los certificados inscritos a través de la aplicación PKI. Esta opción solo es compatible con dispositivos iOS.
UTI schemes	Especifique los esquemas de UTI de la solución PKI basada en aplicación de su empresa. Por ejemplo, si utiliza la aplicación Purebred, use los esquemas siguientes: purebred.zip.all, purebred.zip.no_filter.

Gestión de servicios de aplicaciones de BlackBerry Dynamics

Los servicios de aplicaciones son funciones compartidas que ofrece una aplicación basada en servidor o móvil. Con los SDK de BlackBerry Dynamics, un desarrollador de aplicaciones puede exponer una función de una aplicación que otros desarrolladores pueden usar en sus propias aplicaciones de BlackBerry Dynamics. Con la consola de gestión, puede registrar servicios de aplicaciones para su empresa y proporcionar la definición de los servicios del desarrollador. Los desarrolladores de su empresa pueden proporcionar comentarios sobre los servicios de aplicaciones registradas y pueden aprovechar las definiciones de los servicios disponibles en las aplicaciones de BlackBerry Dynamics que crean.

Los servicios de aplicaciones para determinadas aplicaciones de BlackBerry Dynamics y aplicaciones asociadas también están disponibles para su uso, y las definiciones de los servicios asociados se pueden ver en la consola de gestión. Para obtener más información acerca del desarrollo de servicios de aplicaciones, visite la Comunidad de desarrolladores de BlackBerry Dynamics.

Antes de empezar: Si desea registrar un servicio de aplicaciones para su empresa, compruebe que dispone del ID de servicio de la aplicación, del número de versión y de la definición del servicio.

1. En la consola de gestión, en la barra de menú, haga clic en **Configuración > BlackBerry Dynamics**.
2. Haga clic en **Servicios de aplicaciones**.
3. Lleve a cabo cualquiera de las tareas siguientes:

Tarea	Pasos
Registrar un servicio de aplicaciones para su empresa	**a.** Haga clic en +. **b.** En la lista desplegable **Tipo de servicio**, lleve a cabo una de las acciones siguientes: • Si el servicio de aplicaciones se ofrece mediante una aplicación móvil, haga clic en **Aplicación**. • Si el servicio de aplicaciones se ofrece mediante una aplicación basada en servidor, haga clic en **Servidor**. **c.** En el campo **ID**, escriba el ID del servicio de aplicaciones. El ID debe ser una cadena única (en minúsculas) en notación de DNS inverso (por ejemplo, com.example.service.print). **d.** Escriba un nombre y una descripción para el servicio de aplicaciones. **e.** En el campo **Versión**, escriba la versión. El número de versión debe incluir solo dígitos. Si desea agregar uno o más número de subversiones (por ejemplo, la versión de la compilación), use puntos para separar los segmentos. Los segmentos no pueden empezar con 0 (por ejemplo, 1.1.5 es válido, pero no 1.1.05). **f.** De manera opcional, puede escribir una descripción para la versión. **g.** En el campo **Definición del servicio**, escriba la definición del servicio en formato JSON. **h.** Haga clic en **Save**.
Editar un servicio de aplicaciones	Utilice los siguientes pasos para editar un servicio de aplicaciones que se registró para su empresa (por ejemplo, para añadir una nueva versión). No puede cambiar el tipo de servicio de aplicaciones ni el ID. No puede editar un servicio de aplicaciones de BlackBerry Dynamics o un servicio de aplicaciones asociadas. **a.** Busque el servicio de aplicaciones que desee editar. **b.** Haga clic en el nombre del servicio de aplicaciones. **c.** Edite los detalles del servicio de aplicaciones según sea necesario. Para agregar una nueva versión, haga clic en + y especifique el número de versión, la descripción y la definición del servicio. **Nota:** Eliminar una versión del servicio de aplicaciones no tiene ningún impacto en las aplicaciones que ofrecen o utilizan el servicio, simplemente elimina la definición del servicio de la consola de gestión para que los desarrolladores de su empresa no puedan consultarlo. **d.** Haga clic en **Save**.
Eliminar un servicio de aplicaciones	No puede eliminar un servicio de aplicaciones de BlackBerry Dynamics o un servicio de aplicaciones asociadas. Eliminar un servicio de aplicaciones de la consola de gestión no tiene ningún impacto en las aplicaciones que ofrecen o utilizan el servicio, simplemente elimina la definición del servicio de la consola de gestión para que los desarrolladores de su empresa no puedan consultarlo. **a.** Busque el servicio de aplicaciones que desee eliminar. **b.** Haga clic en × junto al servicio. **c.** Haga clic en **Eliminar**.

Después de terminar: De manera opcional, puede combinar una versión del servicio de aplicaciones con una aplicación gestionada para que la consola de gestión pueda indicar que la aplicación proporciona el servicio. Para obtener más información, consulte Gestión de la configuración de una aplicación de BlackBerry Dynamics.

Configuración de Kerberos para aplicaciones de BlackBerry Dynamics

Las aplicaciones de BlackBerry Dynamics son compatibles con delegación restringida Kerberos y Kerberos PKINIT. Delegación restringida Kerberos (KCD) y Kerberos PKINIT son implementaciones diferentes de Kerberos. Las aplicaciones de BlackBerry Dynamics pueden admitir una o la otra, pero no ambas.

Delegación restringida Kerberos utiliza una relación de confianza establecida previamente entre BlackBerry UEM y el centro de distribución de claves (KDC) de Windows. BlackBerry UEM se comunica con el KDC en nombre de la aplicación. Delegación restringida Kerberos tiene preferencia sobre Kerberos PKINIT, incluso si el usuario tiene un certificado válido. Para obtener información general sobre la delegación restringida Kerberos funciona con las aplicaciones de BlackBerry Dynamics, consulte Delegación restringida Kerberos con Good Control.

La autenticación Kerberos PKINIT establece una confianza directa entre la aplicación BlackBerry Dynamics y el KDC de Windows. La autenticación de usuario se basa en los certificados emitidos por los servicios de certificados de Microsoft Active Directory. Para utilizar PKINIT, la delegación restringida Kerberos no debe estar habilitada en la configuración de la aplicación en BlackBerry UEM.

Configuración de la delegación restringida Kerberos

La delegación restringida Kerberos permite a los usuarios acceder a recursos empresariales sin tener que introducir sus credenciales de red. La delegación restringida Kerberos utiliza vales de servicio que se cifran y descifran mediante claves que no contienen las credenciales del usuario.

Cuando se configura la delegación restringida Kerberos, la aplicación delega la autenticación a BlackBerry UEM para que actúe en su nombre para solicitar acceso a un recurso empresarial.

Configure la delegación restringida Kerberos siguiendo estas directrices:

- Active la autenticación Kerberos (en Autenticación de Windows) para el servidor web de Microsoft Exchange Web Services en Microsoft Internet Information Services (IIS).
- En "Usuarios y equipos de Active Directory" de Microsoft Management Console (MMC), en la pestaña Delegación, agregue el servicio HTTP del servidor web de Microsoft Exchange Web Services a la cuenta de Good Admin.
- Si se activa la delegación restringida Kerberos, los usuarios no pueden introducir sus credenciales de autenticación (nombres de usuario y contraseñas). La autenticación se delega a BlackBerry UEM.

Para activar la delegación restringida Kerberos para una aplicación de BlackBerry Dynamics, seleccione el ajuste **Permitir el uso de delegación restringida Kerberos** en la configuración de la aplicación. Para obtener instrucciones detalladas, consulte el contenido de administración de la aplicación.

Configuración de Kerberos PKINIT

BlackBerry UEM es compatible con Kerberos PKINIT para la autenticación de usuarios de BlackBerry Dynamics mediante certificados PKI.

Si desea utilizar Kerberos PKINIT para las aplicaciones de BlackBerry Dynamics, la empresa debe cumplir los requisitos siguientes:

Puntos clave

- No se debe activar la delegación restringida Kerberos.

- No se debe agregar el host de KDC a la lista Dominios permitidos en el perfil de conectividad de BlackBerry Dynamics.
- El host de KDC debe estar escuchando en el puerto TCP 88 (el puerto predeterminado de Kerberos).
- BlackBerry Dynamics no es compatible con KDC a través de UDP.
- El KDC debe tener un registro A (IPv4) o un registro AAAA (IPv6) en su DNS.
- BlackBerry Dynamics no utiliza archivos de configuración de Kerberos (como `krb5.conf`) para localizar el KDC correcto.
- El KDC puede remitir al cliente a otro host de KDC. BlackBerry Dynamics seguirá la remisión, siempre que el host de KDC al que se remite se agregue a la lista Dominios permitidos en la perfil de conectividad de BlackBerry Dynamics.
- El KDC puede obtener el TGT de forma transparente en BlackBerry Dynamics a partir de otro host de KDC.

Certificados del servidor

- Los certificados de servidor de KDC de Windows emitidos a través de los Servicios de certificados de Active Directory deben provenir únicamente de las siguientes versiones de Windows Server. El resto de versiones del servidor no son compatibles.
  - Internet Information Server con Windows Server 2008 R2
  - Internet Information Server con Windows Server 2012 R2
- Los certificados de servicios de KDC válidos se deben encontrar en el almacén de certificados de BlackBerry Dynamics o el almacén de certificados de dispositivo.

Certificados de cliente

- La longitud de clave mínima de los certificados debe ser 2048 bytes.
- Los certificados de cliente deben incluir el nombre principal del usuario (por ejemplo, usuario@dominio.com) en el nombre alternativo del asunto del ID de objeto szOID_NT_PRINCIPAL_NAME 1.3.6.1.4.1.311.20.2.3, como especifica Microsoft en https://support.microsoft.com/en-us/kb/287547.
- El dominio del nombre principal del usuario debe coincidir con el nombre del dominio del servicio KDC de Windows.
- La propiedad Uso extendido de la clave del certificado debe ser inicio de sesión de tarjeta inteligente de Microsoft (1.3.6.1.4.1.311.20.2.2).
- Los certificados deben ser válidos. Valídelos en los servidores enumerados anteriormente.

Adición del catálogo de aplicaciones de trabajo a BlackBerry Dynamics Launcher

Para los dispositivos que están activados para BlackBerry Dynamics, puede agregar el catálogo de aplicaciones de trabajo a BlackBerry Dynamics Launcher para que los usuarios puedan acceder rápidamente a una lista de sus aplicaciones de trabajo asignadas.

1. En la barra de menú, haga clic en **Grupos**.
2. Seleccione el grupo **Todos los usuarios**.
3. En la sección **Aplicaciones asignadas**, haga clic en +.
4. En el campo de búsqueda, busque **Función: tienda de aplicaciones de BlackBerry**.
5. Seleccione **Función: tienda de aplicaciones de BlackBerry**.
6. En la lista desplegable **Disposición** de la aplicación, seleccione **Necesario**.
7. Haga clic en **Asignar**.

Generación de claves de acceso para aplicaciones de BlackBerry Dynamics

Las aplicaciones de BlackBerry Dynamics requieren una clave de acceso para activarse en un dispositivo. BlackBerry UEM Client puede solicitar las claves de acceso automáticamente desde BlackBerry UEM después de que los usuarios instalen una aplicación. Usted o un usuario deben generar manualmente las claves de acceso y enviarlas para activar las aplicaciones de BlackBerry Dynamics en las situaciones siguientes:

- Para dispositivos Samsung KNOX Workspace
- Para los dispositivos iOS y Android que no necesitan MDM y no tienen UEM Client instalado.
- Para los usuarios que quieran activar aplicaciones de BlackBerry Dynamics en dispositivos que no requieren BlackBerry UEM Client.

Puede generar claves de acceso cuando crea un nuevo usuario o en cualquier momento después. Los usuarios no necesitan activar sus dispositivos en BlackBerry UEM para recuperar claves de acceso. Los usuarios también pueden generar claves de acceso en BlackBerry UEM Self-Service.

1. En la barra de menú, haga clic en **Usuarios > Dispositivos gestionados**.
2. Busque una cuenta de usuario.
3. En los resultados de la búsqueda, haga clic en el nombre de la cuenta de usuario.
4. Haga clic en **Establecer contraseña de activación**.
5. En la lista desplegable **Opción de activación**, seleccione **Generación de clave de acceso de BlackBerry Dynamics**.
6. En la lista desplegable **Número de claves de acceso que se van a generar**, seleccione el número de claves de acceso que desea crear para el usuario.
7. Seleccione el número de días que desea que las claves de acceso sigan siendo válidas.
8. En la lista desplegable **Plantilla de correo**, seleccione la plantilla de correo que desea utilizar. Para obtener más información, consulte Plantillas de correo.
9. Haga clic en **Enviar**.

Gestión de claves de acceso de BlackBerry Dynamics

Tras generar claves de acceso de BlackBerry Dynamics, el número de claves que se ha generado se incluye en los datos de la sección Activación en la pantalla de resumen del usuario.

Antes de empezar: Generación de claves de acceso para aplicaciones de BlackBerry Dynamics.

1. En la barra de menú, haga clic en **Usuarios > Dispositivos gestionados**.
2. Busque una cuenta de usuario.
3. En los resultados de la búsqueda, haga clic en el nombre de la cuenta de usuario.
4. En la sección **Detalles de activación**, en **Claves de acceso de BlackBerry Dynamics**, haga clic en el vínculo que muestra el número de claves generadas. Si no ve esta sección, no se han generado claves de acceso para el usuario.
5. En el cuadro de diálogo **Claves de acceso de BlackBerry Dynamics**, realice una de las siguientes tareas:

Opción	
	Se vuelve a enviar la clave de acceso al usuario.
	Se elimina la clave de acceso.

6. Haga clic en **Guardar**.

Enviar una clave de desbloque de aplicaciones de BlackBerry Dynamics a un usuario

Puede enviar claves de desbloqueo de aplicaciones a un usuario si una de las aplicaciones de BlackBerry Dynamics se han bloqueado.

1. En la barra de menú, haga clic en **Users**.
2. Busque una cuenta de usuario.
3. En los resultados de la búsqueda, haga clic en el nombre de la cuenta de usuario.
4. Haga clic en el dispositivo del usuario.
5. En la sección BlackBerry Dynamics de la fila **Acciones de aplicación**, seleccione "Desbloquear aplicación" para la aplicación para la que desea enviar un correo al usuario.
6. En la página **Desbloquear aplicación**, en el campo **Plantilla de correo**, seleccione el correo de clave de desbloqueo de BlackBerry Dynamics.
7. Haga clic en **Enviar**.

Después de terminar:

Puede editar la plantilla de correo que se envía al usuario.

Gestión de aplicaciones protegida por Microsoft Intune

Microsoft Intune es un servicio EMM basado en la nube que proporciona funciones MDM y MAM. Intune MAM ofrece características de seguridad para las aplicaciones, incluidas las aplicaciones Office 365, que protegen los datos dentro de aplicaciones. Por ejemplo, Intune puede requerir que los datos de las aplicaciones se cifren e impidan copiar y pegar, imprimir y usar el comando Guardar como.

Para dispositivos iOS y Android, si desea utilizar políticas de protección de aplicaciones Intune para proteger datos en aplicaciones Office 365, puede hacerlo mientras utiliza BlackBerry UEM para gestionar los dispositivos. Puede conectar UEM a Intune, lo que le permite establecer políticas de protección de aplicaciones Intune desde dentro de la consola de administración de UEM.

Para implementar aplicaciones protegidas por Intune, primero debe configurar la conexión entre UEM y Intune. Para obtener más información, consulte Conexión de BlackBerry UEM a Microsoft Azureen el contenido referente a Configuración.

Intune utiliza políticas de protección de aplicaciones para proteger aplicaciones. Para proteger aplicaciones de la consola de gestión de UEM, cree un perfil de protección de aplicaciones de Intune. Cuando crea o actualiza un perfil de protección de la aplicación en UEM, la configuración se envía a Intune y actualiza la configuración en la política de protección de la aplicación correspondiente.

Nota: Si actualiza la política de protección de aplicaciones en Intune, los cambios no se sincronizarán con BlackBerry UEM. Después de crear un perfil de protección de aplicaciones en UEM, no actualice la directiva correspondiente desde Intune.

Creación de un perfil de protección de aplicación de Microsoft Intune

Cuando crea o actualiza un perfil de protección de la aplicación Microsoft Intune en BlackBerry UEM, la configuración se envía a Intune y actualiza la política de protección de la aplicación correspondiente. Microsoft Intune Los perfiles de protección de la aplicación <1/> se pueden asignar únicamente a grupos vinculados a directorios.

Antes de empezar:

- Configurar la conexión entre BlackBerry UEM y Microsoft Intune. El perfil de protección de la aplicación Microsoft Intune no aparece en la página de Políticas y perfiles si la conexión no está configurada.

- Para los dispositivos Android, asegúrese de que la aplicación Portal de la empresa Microsoft está instalada en los dispositivos. Para obtener más información, consulte https://docs.microsoft.com/intune/app-protection-enabled-apps-android.

1. En la barra de menú, haga clic en **Políticas y perfiles**.
2. Haga clic en **Protección > Perfil de protección de aplicaciones de Microsoft Intune**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil.
5. Configure los valores adecuados para cada tipo de dispositivo.
6. Haga clic en **Agregar**.

Después de terminar: Asigne el perfil de protección de la aplicación Intune a un grupo vinculado a directorios.

Conceptos relacionados

Configuración del perfil de protección de aplicaciones de Microsoft Intune

Tareas relacionadas

Asignación de un perfil o una política de TI a un grupo de usuarios

Borrar aplicaciones gestionadas por Microsoft Intune

Puede utilizar el comando Limpiar aplicaciones para eliminar los datos de las aplicaciones gestionadas por Intune en dispositivos iOS y Android. Las aplicaciones no se desinstalan al enviar el comando.

1. En la barra de menú, haga clic en **Users**.
2. Busque al usuario del que desea borrar los datos y haga clic en él.
3. Haga clic en la pestaña **<*modelo de dispositivo*> (Intune)**.
4. Haga clic en **Limpiar aplicaciones**.

Gestión de las cuentas de VPP de Apple

El programa de compras por volumen (VPP) Apple le permite adquirir, distribuir y actualizar grandes cantidades de aplicaciones instaladas iOS. Puede vincular cuentas de VPP de Apple a BlackBerry UEM de modo que sea posible distribuir licencias adquiridas para las aplicaciones de iOS asociadas a las cuentas de VPP.

Adición de una cuenta de VPP de Apple

Para ver cómo se agrega una cuenta de VPP de Apple, visite nuestro canal de YouTube.

1. En la barra de menús, haga clic en **Aplicaciones > Licencias de la aplicación de iOS**.
2. Haga clic en **Agregar una cuenta de Apple VPP**.
3. Escriba el nombre y la información del titular de la cuenta de la cuenta de VPP.
4. En el campo **Identificador de servicio de VPP**, copie y pegue el código de 64 bits desde el archivo del identificador .vpp. Es el archivo que el titular de la cuenta de VPP ha descargado de la tienda de VPP.
5. Haga clic en **Siguiente**.
6. Seleccione las aplicaciones que desea agregar a la lista de aplicaciones. Si una aplicación ya se ha agregado a la lista de aplicaciones, no se puede seleccionar.

7. Si desea que las aplicaciones se actualicen automáticamente cuando esté disponible una versión actualizada en BlackBerry UEM, seleccione **Actualizar automáticamente la aplicación cuando haya disponible una nueva versión**. Este valor se aplica a todas las aplicaciones VPP para esta cuenta VPP. Puede modificar este valor más tarde.
8. Si desea que las aplicaciones se eliminen de los dispositivos cuando estas se hayan eliminado de BlackBerry UEM, seleccione **Eliminar la aplicación del dispositivo cuando este se haya eliminado del sistema**.
9. Para evitar que las aplicaciones en dispositivos iOS realicen la copia de seguridad en el servicio en línea iCloud, seleccione **Desactivar copia de seguridad en iCloud para la aplicación**. Esta opción se aplica únicamente cuando la disposición de la aplicación se establece como obligatoria. La disposición de la aplicación se establece al asignarse a un usuario o grupo.
10. En la lista desplegable **Método de instalación predeterminado**, lleve a cabo una de las siguientes acciones:
    - Seleccione **Preguntar una vez** si desea que los usuarios reciban una solicitud para instalar las aplicaciones en sus dispositivos iOS. Si los usuarios descartan la solicitud, pueden instalar las aplicaciones más adelante mediante la lista Aplicaciones de trabajo en la aplicación BlackBerry UEM Client o en el icono Aplicaciones de trabajo del dispositivo.
    - Seleccione **No preguntar**. No se notificará a los usuarios. Pueden instalar las aplicaciones mediante la lista Aplicaciones de trabajo en la aplicación BlackBerry UEM Client o en el icono Aplicaciones de trabajo del dispositivo.
11. Haga clic en **Agregar**.

Tareas relacionadas

Asignación de una aplicación a un grupo de usuarios
Asignación de una aplicación a una cuenta de usuario

Edición de una cuenta de VPP de Apple

1. En la barra de menús, haga clic en **Aplicaciones > Licencias de la aplicación de iOS**.
2. Haga clic en .
3. Edita la configuración de la información de la cuenta VPP:
    - Nombre de la cuenta de VPP
    - Información del titular de la cuenta de VPP
    - Identificador de servicio de VPP
    - Actualizar automáticamente la aplicación cuando haya disponible una nueva versión.
4. Haga clic en **Guardar**.

Actualización de la información de la cuenta de VPP de Apple

Cuando se abre la página Licencias de la aplicación, la mayoría de la información de licencias más reciente se sincroniza automáticamente desde los servidores de VPP de Apple. Si es necesario, también puede actualizar manualmente la información de licencias que haya agregado a BlackBerry UEM.

1. En la barra de menús, haga clic en **Aplicaciones**.
2. Haga clic en **Licencias de la aplicación de iOS**.
3. Haga clic en .

Eliminación de una cuenta de VPP de Apple

Antes de empezar: Elimine las aplicaciones que tengan licencias asociadas de los usuarios o antes de eliminar la cuenta de VPP.

1. En la barra de menús, haga clic en **Aplicaciones**.
2. Haga clic en **Licencias de la aplicación de iOS**.
3. Haga clic en .
4. Haga clic en **Eliminar**.

Asignación de licencias VPP de Apple a los dispositivos

Puede asignar licencias Volume Purchase Program (VPP) de Apple a los dispositivos que ejecuten con iOS 9 y posteriores. La asignación de licencias VPP a los dispositivos en lugar de a los usuarios simplifica el proceso para los usuarios, porque ya no necesitan un ID de Apple para instalar aplicaciones. Además, las aplicaciones no aparecen en el historial de compras y las instalaciones de aplicaciones de los usuarios. Al cambiar el tipo de asignación existente para una aplicación de asignada al usuario a asignada al dispositivo, el usuario debe reinstalar la aplicación antes de que se aplique la nueva asignación y se muestre en la consola de administración de BlackBerry UEM.

La asignación de licencias VPP a dispositivos solo es compatible en dispositivos iOS activados con Controles de MDM.

Puede asignar licencias VPP a dispositivos cuando se agregan aplicaciones a cualquiera de los siguientes grupos y cuentas:

- Cuentas de usuario
- Grupos de aplicaciones
- Grupos de usuarios

La asignación de licencias VPP a grupos de dispositivos no es compatible.

Para obtener más información, consulte Gestión de las cuentas de VPP de Apple.

Visualice la asignación de licencias VPP de Apple

Puede ver el estado de la asignación de licencias VPP Apple en su dominio.

1. En la barra de menús, haga clic en **Aplicaciones** > **Licencias de la aplicación de iOS**.
2. Si dispone de más de una cuenta VPP de Apple, haga clic en la cuenta VPP de la que desee ver la asignación de licencias VPP.

   Para cada aplicación de iOS en el dominio, puede ver la siguiente información de licencia VPP:

   - El número de licencias VPP disponibles
   - El número de licencias VPP utilizadas
3. En la columna **Licencias utilizadas** de la aplicación, haga clic en el vínculo de licencias utilizadas.

   Para la aplicación especificada, puede ver la siguiente información de asignación de licencias de aplicaciones:

   - Los nombres de usuario para los que tiene la licencia la aplicación
   - Si la licencia de la aplicación está asignada a una cuenta de usuario o a un dispositivo
   - Si se utiliza o no una licencia VPP
   - Si la aplicación está instalada o no
4. Haga clic en **Cerrar**.

Clasificar la instalación de aplicaciones

Puede clasificar las aplicaciones para controlar el orden en el que se instalan al asignarlas a dispositivos. La configuración de la clasificación garantiza que las aplicaciones delegadas de la autenticación se inserten en el dispositivo primero. La clasificación se aplica solo a las aplicaciones de iOS.

1. En la barra de menú, haga clic en **Aplicaciones > Clasificación de instalación de aplicaciones**.
2. Haga clic en .
3. Haga clic en .
4. Haga clic en la casilla de verificación situada junto a las aplicaciones que desea clasificar.
5. Haga clic en **Agregar**.
6. En la página Clasificación de instalación de aplicaciones, haga clic en en la columna **Clasificación** para colocar las aplicaciones en el orden en que desea que se instalen en los dispositivos.
7. Haga clic en **Guardar**.

Editar la lista de clasificación de instalación de aplicaciones

Puede editar la secuencia de instalación de las aplicaciones que se instalarán en los dispositivos de su empresa. La clasificación se aplica solo a las aplicaciones de iOS.

1. En la barra de menú, haga clic en **Aplicaciones > Clasificación de instalación de aplicaciones**.
2. Haga clic en .
3. Haga clic en en la columna **Clasificación** para colocar las aplicaciones en el orden en que desea que se instalen en los dispositivos.
4. Haga clic en **Guardar**.

Eliminar una aplicación de la lista de clasificación de instalación de aplicaciones

Puede eliminar una aplicación de la lista de clasificación de instalación de aplicaciones. La clasificación se aplica solo a las aplicaciones de iOS.

1. En la barra de menú, haga clic en **Aplicaciones > Clasificación de instalación de aplicaciones**.
2. Haga clic en .
3. En la lista, haga clic en junto a la aplicación que desea eliminar.
4. Haga clic en **Eliminar**.
5. Haga clic en **Guardar**.

Visualización de las listas de aplicaciones personales

De forma predeterminada, BlackBerry UEM recibe una lista de las aplicaciones personales que están instaladas en los dispositivos activados con un tipo de activación admitido.

En la consola de gestión de BlackBerry UEM, puede consultar la lista de aplicaciones personales en la página de detalles del dispositivo para una cuenta de usuario específica, o en la página de aplicaciones personales para todas las cuentas de usuario. Consulte Visualización de la lista de aplicaciones personales en la consola de gestión.

Nota: También puede ver las aplicaciones instaladas en los dispositivos antes de que se activen como dispositivos de solo KNOX Workspace.

La visualización de la lista de aplicaciones personales no es compatible con los dispositivos que están activados con los tipos de activación siguientes:

- iOS y Android: Privacidad del usuario
- Android: Trabajo y personal: privacidad de usuario
- Samsung KNOX: Trabajo y personal: privacidad de usuario - (Samsung KNOX)
- BlackBerry 10: Trabajo y personal - Empresa
- iOS y Android: registro de dispositivo solo para BlackBerry 2FA

Para desactivar la recopilación de aplicaciones personales para todos los tipos de activación, debe desmarcar la opción "Permitir recopilaciones de aplicaciones personales" en el perfil de Enterprise Management Agent. Para obtener más información, consulte Desactivación de la recopilación de aplicaciones personales.

Visualización de la lista de aplicaciones personales en la consola de gestión

Puede ver la siguiente información acerca de las aplicaciones que están instaladas en el espacio personal del usuario:

- Nombre de la aplicación
- Versión de la aplicación
- SO compatible con la aplicación
- Número de cuentas de usuario que tienen la aplicación instalada

Antes de empezar: Cree un perfil de activación con un tipo de activación que sea compatible con BlackBerry UEM, que recibirá una lista de aplicaciones que se instalan en el espacio personal del usuario y se asigna a grupos y usuarios.

1. En la barra de menús, haga clic en **Aplicaciones > Aplicaciones personales**.
2. En la columna **Nombre de la aplicación**, haga clic en el nombre de la aplicación.

   Para la aplicación especificada, puede ver los detalles de la aplicación correspondiente en la tienda de aplicaciones públicas, cuando proceda.
3. En la columna **N.º instalado** de la aplicación, haga clic en el número instalado.

   Para la aplicación especificada, puede ver la cuenta de usuario y el dispositivo en el que está instalada la aplicación.

Desactivación de la recopilación de aplicaciones personales

De forma predeterminada, BlackBerry UEM recibe una lista de las aplicaciones personales que están instaladas en los dispositivos activados con un tipo de activación admitido. Puede desactivar la recopilación de aplicaciones personales para todos los tipos de activación.

1. En la barra de menú, haga clic en **Políticas y perfiles**.
2. Expanda **Enterprise Management Agent**.
3. Haga clic en el nombre del perfil que desea cambiar.
4. Haga clic en .
5. Desactive la casilla de verificación **Permitir recopilaciones de aplicaciones personales** correspondiente a cada uno de los tipos de dispositivo.
6. Haga clic en **Guardar**.

Valoración y comentarios relativos a aplicaciones

Puede especificar si los usuarios de su empresa pueden valorar y proporcionar comentarios de aplicaciones de iOS, Android y Windows 10, y ver comentarios de otros usuarios sobre aplicaciones personalizadas internas o aplicaciones que se descargan desde tiendas de aplicaciones públicas. Otros usuarios fuera de su entorno no pueden ver las valoraciones y los comentarios enviados sobre las aplicaciones. Los comentarios pueden contener un máximo de 1000 caracteres.

Los usuarios pueden valorar una aplicación sin proporcionar un comentario, pero deben valorar la aplicación cuando proporcionen un comentario. Las valoraciones y comentarios enviados por usuarios se guardan y se pueden ver en la consola de BlackBerry UEM casi en tiempo real. Puede ver la valoración media de una aplicación, el número de comentarios enviados y leer los comentarios individuales sobre la aplicación. También puede eliminar las valoraciones y los comentarios según sea necesario.

Cuando agrega varias versiones de una aplicación personalizada a BlackBerry UEM y permite la valoración y los comentarios sobre una versión de la aplicación, la configuración especificada se aplica a todas las versiones de la aplicación personalizada. La valoración media y el recuento de comentarios, así como la valoración y los comentarios de aplicaciones enviados sobre diferentes versiones de la aplicación personalizada muestran la misma información para cada versión.

De forma predeterminada, las nuevas aplicaciones agregadas a la lista de aplicaciones en la consola de gestión de BlackBerry UEM permiten a los usuarios valorar la aplicación, proporcionar comentarios de la aplicación y ver comentarios proporcionados por otros usuarios en su empresa. De manera predeterminada, la opción valoración y comentarios de la aplicación se desactiva para aplicaciones existentes, pero puede activar esta función según sea necesario. Cuando se activa la opción de valoración y comentarios para una aplicación, el permiso se aplica a cualquier versión de la aplicación que se haya agregado a BlackBerry UEM.

La opción de valoración y comentarios de aplicaciones no es compatible en los siguientes dispositivos:

- BlackBerry
- Windows 8.x
- Con BlackBerry Dynamics
- Dispositivos Android que utilizan un perfil de trabajo
- BlackBerry Enterprise Identity

Para obtener más información sobre BlackBerry Enterprise Identity, consulte el contenido de BlackBerry Enterprise Identity.

Activar o desactivar las valoraciones y los comentarios para todas las aplicaciones

Puede activar o desactivar las valoraciones y los comentarios para todas las aplicaciones que haya agregado a BlackBerry UEM y configurar el nivel de interacción que puede tener un usuario con los comentarios y las valoraciones.

Nota: Los ajustes de valoración y comentarios de aplicaciones se aplican únicamente a aplicaciones agregadas después de guardar la configuración.

1. En la barra de menú, haga clic en **Configuración > Administración de aplicaciones**.
2. Haga clic en **Valoraciones y comentarios**.
3. Para activar las valoraciones y los comentarios de aplicaciones, seleccione **Activar valoraciones y comentarios de la aplicación**.
    - Si desea que los usuarios puedan valorar y proporcionar comentarios de la aplicación, así como leer comentarios enviados por otros usuarios en su entorno, seleccione **Modo público**.

- Si desea que los usuarios solo valoren y proporcionen comentarios de aplicaciones, seleccione **Modo privado**. Los usuarios no pueden ver los comentarios proporcionados por otros usuarios. Puede ver comentarios en la consola de gestión de BlackBerry UEM.
- Si no desea que los usuarios valoren o proporcionen comentarios de aplicaciones o vean los comentarios proporcionados por otros usuarios, seleccione **Desactivado**.

4. Para desactivar las valoraciones y los comentarios de aplicaciones, suprima **Activar valoraciones y comentarios de la aplicación**.
5. Haga clic en **Guardar**.

Activación de la opción de valoración y comentarios para aplicaciones existentes

Cuando especifique si los usuarios pueden valorar una aplicación, proporcionar comentarios de una aplicación y ver los comentarios proporcionados por otros usuarios, el permiso especificado se aplica a todas las versiones de la aplicación.

1. En la barra de menú, haga clic en **Aplicaciones**.
2. Haga clic en una aplicación.
3. En la pestaña **Configuración**, en la lista desplegable **Valoración y comentarios de aplicaciones**, realice una de las siguientes acciones:
   - Si desea que los usuarios puedan valorar y proporcionar comentarios de la aplicación, así como leer comentarios enviados por otros usuarios en su entorno, seleccione **Modo público**.
   - Si desea que los usuarios solo valoren y proporcionen comentarios de aplicaciones, seleccione **Modo privado**. Los usuarios no pueden ver los comentarios proporcionados por otros usuarios. Puede ver comentarios en la consola de gestión de BlackBerry UEM.
   - Si no desea que los usuarios valoren o proporcionen comentarios de aplicaciones o vean los comentarios proporcionados por otros usuarios, seleccione **Desactivado**.
4. Haga clic en **Guardar**.

Visualización de comentarios de aplicaciones en la consola de gestión

Puede ver la valoración media global para una aplicación, así como las valoraciones individuales y comentarios proporcionados por los usuarios de una aplicación.

1. En el menú, haga clic en **Aplicaciones**.
2. De manera opcional, haga clic en la columna **Valoración de la aplicación** para ordenar aplicaciones con la opción activada de valoración y comentarios.

   Las aplicaciones con la opción activada de valoración y comentarios aparecen en el siguiente orden:

   a. Aplicaciones con la opción de valoración y comentarios
   b. Aplicaciones sin la opción de valoración y comentarios
   c. La opción de valoración de la aplicación está desactivada
   d. Aplicaciones que no son compatibles con la opción de valoración y comentarios
3. Haga clic en una aplicación.
4. Haga clic en la pestaña **<*número de comentario*> Comentarios**.

Especificación de la configuración de valoración y comentarios para varias aplicaciones

Cuando especifique si los usuarios pueden valorar una aplicación, proporcionar comentarios de una aplicación y ver los comentarios proporcionados por otros usuarios, el permiso especificado se aplica a todas las versiones de la aplicación.

1. En el menú, haga clic en **Aplicaciones**.
2. Lleve a cabo una de las siguientes acciones:

- Seleccione la casilla de verificación en la parte superior de la lista de aplicaciones para seleccionar todas las aplicaciones.
- Seleccione la casilla de verificación para cada aplicación para la que desee activar la opción de valoración y comentarios de aplicaciones.

3. Haga clic en .
4. Seleccione uno de los siguientes permisos:
   - Si desea que los usuarios puedan valorar y proporcionar comentarios de la aplicación, así como leer comentarios enviados por otros usuarios en su entorno, seleccione **Modo público**.
   - Si desea que los usuarios solo valoren y proporcionen comentarios de aplicaciones, seleccione **Modo privado**; los usuarios no podrán ver comentarios de otros usuarios. Puede ver comentarios en la consola de gestión de BlackBerry UEM.
   - Si no desea que los usuarios valoren o proporcionen comentarios de aplicaciones ni vean los comentarios proporcionados por otros usuarios, seleccione **Desactivado**.
5. Haga clic en **Guardar**.

Eliminar clasificaciones y comentarios sobre la aplicación

Puede eliminar las valoraciones y los comentarios de aplicaciones según sea necesario.

1. En el menú, haga clic en **Aplicaciones**.
2. De manera opcional, haga clic en la columna **Valoración de la aplicación** para ordenar aplicaciones con la opción activada de valoración y comentarios.
3. Haga clic en una aplicación con la opción de valoración y comentarios activada.
4. En la pantalla **Detalles de la aplicación**, haga clic en la pestaña **<*número de comentario*> Comentarios**.
5. Haga clic en **Seleccionar todo** o seleccione la casilla de verificación correspondiente a cada comentario que desee eliminar.
6. Haga clic en .
7. Haga clic en **Eliminar**.
8. Haga clic en **Guardar**.

Gestión del icono Work Apps para los dispositivos iOS

Cuando los usuarios activan los dispositivos iOS con cualquiera de los tipos de activación "Controles de MDM" o "Trabajo y personal: control total", se muestra el icono Aplicaciones de trabajo en el dispositivo. Los usuarios pueden tocar el icono para ver las aplicaciones de trabajo que se les han asignado, y se pueden instalar o actualizar las aplicaciones según sea necesario.

Puede personalizar la apariencia del icono Aplicaciones de trabajo seleccionando una imagen y un nombre para el icono. El nombre predeterminado para el icono Aplicaciones de trabajo es "Aplicaciones de trabajo" y el icono predeterminado muestra un logotipo de BlackBerry.

Personalización del icono Aplicaciones de trabajo

Cuando se personaliza el icono Aplicaciones de trabajo, el icono se actualiza en todos los dispositivos iOS activados.

Nota: Esta función no es compatible con los dispositivos activados con privacidad de usuario.

Antes de empezar: Verifique que la imagen que está pensando utilizar para el icono Aplicaciones de trabajo cumpla los siguientes requisitos:

- El formato de la imagen debe ser .png, .jpg o .jpeg.
- Evite el uso de imágenes .png que tienen elementos transparentes. Los elementos transparentes se muestran como negro en el dispositivo.
- Para saber cuáles son las sugerencias de tamaños de imagen, visite developer.apple.com para consultar los tamaños de los iconos y las imágenes.

1. En la barra de menús, haga clic en **Configuración**.
2. En el panel izquierdo, amplíe **Administración de aplicaciones**.
3. Haga clic en **Aplicación Work Apps para iOS**.
4. En el campo **Nombre**, escriba un nombre para el icono personalizado. El nombre aparece en el dispositivo justo debajo del icono.
5. Haga clic en **Examinar**. Localice y seleccione una imagen para el icono Aplicaciones de trabajo. Los formatos de imagen compatibles son .png, .jpg, .jpeg.
6. Seleccione **Mostrar la aplicación Work Apps en modo de pantalla completa** para que los usuarios puedan cambiar el icono Work Apps del modo normal al de pantalla completa.
7. Haga clic en **Guardar**.

Desactivación de la aplicación Work Apps para iOS

Si los usuarios acceden al catálogo de aplicaciones de trabajo desde BlackBerry Dynamics Launcher, puede desactivar la aplicación Work Apps.

1. En la barra de menú, haga clic en **Settings (Configuración)**.
2. En el panel izquierdo, amplíe **Administración de aplicaciones**.
3. Haga clic en **Aplicaciones de trabajo para iOS**.
4. Haga clic en **Desactivar la aplicación Work Apps**.

Gestión de notificaciones para aplicaciones en dispositivos iOS supervisados

Puede utilizar perfiles de notificación por aplicación para configurar los ajustes de notificación para las aplicaciones del sistema y las aplicaciones que gestiona mediante BlackBerry UEM. Los perfiles de notificación por aplicación son compatibles para los dispositivos supervisados iOS con iOS 9.3 o posterior.

Nota: Debe asignar un perfil de notificación por aplicación a las cuentas de usuario cuando las aplicaciones afectadas se hayan instalado en los dispositivos de los usuarios. Si se aplica el perfil antes de que se instalen las aplicaciones afectadas, puede que los usuarios no puedan activar las notificaciones de las aplicaciones.

Crear perfil de notificación por aplicación

Antes de empezar: Compruebe que las aplicaciones para las que desea configurar ajustes de notificación ya estén instaladas en los dispositivos de los usuarios antes de asignar el perfil de notificación por aplicación. Si se aplica el perfil a dispositivos antes de instalar las aplicaciones correspondientes, es posible que los usuarios no puedan activar las notificaciones para las aplicaciones.

1. En la barra de menú, haga clic en **Políticas y perfiles**.
2. Haga clic en **Personalizada > Notificación por aplicación**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil.

5. En la sección **Configuración de las notificaciones por aplicación**, haga clic en +. Lleve a cabo una de las siguientes acciones para especificar la aplicación para la que desea configurar la configuración de notificaciones:
   - Para seleccionar la aplicación desde la lista de aplicaciones gestionadas, haga clic en **Seleccionar aplicaciones de la lista de aplicaciones**. Busque y seleccione la aplicación.
   - Para especificar la aplicación por su ID de paquete, haga clic en **Agregar un identificador de paquete de la aplicación**. Escriba el nombre de la aplicación y el identificador de paquete.
6. Haga clic en **Siguiente**.
7. Haga clic en **Activar alerta crítica** si desea que las alertas críticas anulen el perfil de no molestar y la configuración de notificaciones de su empresa. Esta configuración se aplica únicamente a dispositivos con iOS 12.0 o versiones posteriores.
8. En la lista desplegable **Notificación** haga clic en **Activado**.
9. Seleccione alguna de las siguientes opciones de notificación:
   - **Mostrar en el centro de notificaciones**
   - **Mostrar en la pantalla de bloqueo**
10. En la lista desplegable **Tipo de alerta de notificación**, seleccione una de las opciones siguientes:
    - **Ninguno**: los usuarios del dispositivo no reciben alertas de notificación.
    - **Banner**: los usuarios del dispositivo reciben alertas de notificación en el banner.
    - **Alerta de modo**: los usuarios del dispositivo reciben alertas de notificación de modo.
11. Seleccione alguna de las siguientes opciones de alerta de notificación:
    - **Activar distintivos**: especifique si desea que la aplicación muestre un distintivo.
    - **Activar sonidos**: especifique si desea que la aplicación emita un sonido.
    - **Mostrar en CarPlay**: especifique si desea que se muestren notificaciones en CarPlay. Esta configuración se aplica únicamente a dispositivos con iOS 12.0 o versiones posteriores.
12. Haga clic en **Guardar**.
13. Repita los pasos del 4 al 9 para agregar más notificaciones por aplicación.
14. Haga clic en **Agregar**.

Después de terminar:

- Para editar los ajustes de notificación para una aplicación, en la sección **Configuración de las notificaciones por aplicación**, haga clic en la configuración de notificaciones de la aplicación y cambie la configuración según sea necesario.
- Si ha creado más de un perfil de notificación por aplicación, clasifique los perfiles.

Tareas relacionadas

Asignación de un perfil o una política de TI a un grupo de usuarios
Asignar un perfil o una política de TI a una cuenta de usuario

Establezca el nombre de la empresa para BlackBerry World

Puede agregar el nombre de la empresa a la tienda de aplicaciones corporativas BlackBerry World para el trabajo.

1. En la barra de menús, haga clic en **Configuración**.
2. Amplíe la **Administración de aplicaciones** y haga clic en **BlackBerry World para el trabajo**.
3. En el campo **Nombre de la empresa**, introduzca el nombre de la empresa.

4. Haga clic en **Guardar**.

Administración de aplicaciones en dispositivos con BlackBerry OS

Si el dominio de BlackBerry UEM admite los dispositivos BlackBerry OS (de la versión 5.0 a la 7.1), puede utilizar la consola de gestión para instalar y gestionar BlackBerry Device Software y las aplicaciones BlackBerry Java Applications en los dispositivos con BlackBerry OS.

Para enviar aplicaciones BlackBerry Java Applications a los dispositivos con BlackBerry OS, primero debe agregar las aplicaciones a la carpeta de red compartida. Puede utilizar la carpeta de red compartida para guardar y administrar todas las versiones de las aplicaciones BlackBerry Java Applications que desea instalar, actualizar o eliminar de los dispositivos.

En la consola de gestión, debe crear configuraciones de software para especificar las versiones de BlackBerry Device Software y de las aplicaciones BlackBerry Java Applications que desea instalar, actualizar o eliminar de los dispositivos con BlackBerry OS. También puede utilizar las configuraciones de software para especificar las aplicaciones que son necesarias, opcionales o no están admitidas. Al crear una configuración de software, también debe especificar si los usuarios pueden instalar las aplicaciones que no se indican en la configuración de software.

Al agregar una aplicación BlackBerry Java Application a una configuración de software, debe asignar una política de control de aplicaciones a las aplicaciones para especificar a qué recursos puede obtener acceso la aplicación. Puede utilizar las políticas de control de aplicaciones predeterminadas o puede crear y utilizar políticas de control de aplicaciones personalizadas. Si permite a los usuarios instalar las aplicaciones que no están indicadas, tendrá que crear una política de control de aplicaciones para las aplicaciones que no se encuentran indicadas que especifique a qué recursos pueden acceder las aplicaciones.

Al asignar una configuración de software a un grupo de usuarios o a cuentas de usuario individuales, la consola de gestión crea un trabajo de implementación para instalar BlackBerry Device Software y las aplicaciones BlackBerry Java Applications en los dispositivos y para aplicar políticas de control de aplicaciones a los dispositivos.

Para obtener más información acerca de la instalación y administración de BlackBerry Device Software en los dispositivos con BlackBerry OS, descargue la guía de actualización de BlackBerry Device Software en help.blackberry.com/detectLang/bes5.

Preparar la distribución de aplicaciones BlackBerry Java Applications

Para enviar una aplicación BlackBerry Java Application a los dispositivos con BlackBerry OS (de la versión 5.0 a la 7.1), el desarrollador de la aplicación debe crear un archivo .zip que contenga los archivos de aplicación necesarios y un archivo .alx que contenga información acerca de la aplicación. Si una estructura de directorios está descrita en el archivo .alx, dicha estructura de directorios debe estar representada en el archivo .zip.

Antes de distribuir aplicaciones BlackBerry Java Application, debe especificar una carpeta de red compartida para las aplicaciones BlackBerry Java Application mediante la consola de gestión. Para obtener más información, consulte Especificación de la ubicación de red compartida para guardar aplicaciones internas.

Después de agregar una aplicación a la carpeta de red compartida, puede agregar la aplicación a una configuración de software, especificar si la aplicación es obligatoria, opcional o no está permitida en los dispositivos con BlackBerry OS y asignar una política de control de aplicaciones a la aplicación para controlar los permisos de acceso para la aplicación. Las configuraciones de software se asignan a cuentas de usuario para instalar o actualizar las aplicaciones BlackBerry Java Applications en dispositivos BlackBerry o para eliminar aplicaciones BlackBerry Java Application de dispositivos con BlackBerry OS.

Adición de una aplicación BlackBerry Java Application a la carpeta de red compartida

Para enviar una aplicación BlackBerry Java Application a los dispositivos con BlackBerry OS (de la versión 5.0 a la 7.1), primero debe agregar el paquete de la aplicación BlackBerry Java Application a la ubicación de red compartida. Para enviar una versión actualizada de una aplicación BlackBerry Java Application a dispositivos con BlackBerry OS, debe agregar antes el paquete actualizado al repositorio de aplicaciones. Para obtener más información acerca de la configuración de una carpeta compartida de red, consulte Especificación de la ubicación de red compartida para guardar aplicaciones internas.

1. En la barra de menús, haga clic en **Configuración de BlackBerry OS**.
2. Haga clic en **Agregar o actualizar aplicaciones**.
3. En la sección **Ubicación de la aplicación**, haga clic en **Examinar**. Vaya al paquete de la aplicación BlackBerry Java Application que desee agregar o actualizar al repositorio de aplicaciones.
4. Haga clic en **Siguiente**.
5. Haga clic en **Agregar aplicación**.

Especificación de palabras clave para una aplicación BlackBerry Java Application

Puede especificar palabras clave para una aplicación BlackBerry Java Application. Puede utilizar las palabras clave para buscar la aplicación en el repositorio de aplicaciones.

1. En la barra de menús, haga clic en **Configuración de BlackBerry OS**.
2. Haga clic en **Administrar aplicaciones**.
3. Busque una aplicación.
4. En los resultados de la búsqueda, haga clic en el nombre de una aplicación.
5. Haga clic en **Editar aplicación**.
6. En el campo **Palabras clave de la aplicación**, introduzca una palabra clave.
7. Haga clic en el icono **Agregar**.
8. Repita los pasos 6 y 7 para cada palabra clave que desee agregar.
9. Haga clic en **Guardar todo**.

Configuración de las políticas de control de aplicaciones

Cuando agrega una aplicación BlackBerry Java Application a una configuración de software para poder instalar la aplicación en dispositivos con BlackBerry OS (de la versión 5.0 a la 7.1), debe especificar la política de control de aplicaciones que desea aplicar a la aplicación BlackBerry Java Application. Las políticas de control de aplicaciones controlan los datos y las API a los que las aplicaciones BlackBerry Java Applications pueden acceder en los dispositivos con BlackBerry OS, así como las fuentes de datos externos y conexiones de red a las que las aplicaciones BlackBerry Java Applications pueden acceder.

BlackBerry UEM incluye una política estándar de control de aplicaciones para aplicaciones BlackBerry Java Applications que se clasifica como obligatoria, opcional o no permitida. Puede cambiar la configuración predeterminada de las políticas de control de aplicaciones estándar o crear políticas de control de aplicaciones personalizadas para una aplicación BlackBerry Java Application.

Para obtener más información acerca de cómo configurar los ajustes de las reglas de política de control de aplicaciones, descargue la Guía de referencia de políticas en help.blackberry.com/detectLang/bes5.

Políticas estándar de control de aplicaciones

BlackBerry UEM incluye las siguientes políticas estándar de control de aplicaciones para dispositivos con BlackBerry OS (de la versión 5.0 a la 7.1).

Política de control de aplicaciones	Descripción
Estándar necesario	Cuando se aplica la política de control de aplicaciones a una aplicación BlackBerry Java Application, la configuración de la regla requiere que esté instalada la aplicación BlackBerry Java Application y que se permita su ejecución en los dispositivos con BlackBerry OS.Los dispositivos con BlackBerry OS instalan la aplicación automáticamente.
Estándar opcional	Cuando se aplica la política de control de aplicaciones a una aplicación BlackBerry Java Application, la configuración de la regla establece la aplicación BlackBerry Java Application como opcional en el dispositivo con BlackBerry OS. Los usuarios pueden instalar y ejecutar la aplicación BlackBerry Java Application en sus dispositivos con BlackBerry OS.
Estándar no permitido	Cuando se aplica la política de control de aplicaciones a una aplicación BlackBerry Java Application, la configuración de la regla impide que los usuarios instalen la aplicación BlackBerry Java Application en dispositivos con BlackBerry OS. Los usuarios no pueden instalar y ejecutar la aplicación BlackBerry Java Application en sus dispositivos con BlackBerry OS.

Cambiar una política estándar de control de aplicaciones

Cuando se agrega una aplicación BlackBerry Java Application a una configuración de software, debe asignar una política de control de aplicaciones a BlackBerry Java Application. Basándose en los requisitos del entorno de la empresa, puede cambiar la configuración predeterminada para las políticas de control de aplicaciones estándar.

1. En la barra de menús, haga clic en **Configuración de BlackBerry OS**.
2. Haga clic en **Gestionar políticas de control de aplicaciones predeterminadas**.
3. Haga clic en la política estándar de control de aplicaciones que desea cambiar.
4. Haga clic en **Editar política de control de aplicaciones**.
5. En la pestaña **Configuración de acceso**, en la sección **Configuración**, cambie la configuración de la política estándar de control de aplicaciones.
6. Haga clic en **Guardar todo**.

Creación de políticas personalizadas de control de aplicaciones para una BlackBerry Java Application

Una vez que agregue una aplicación BlackBerry Java Application a la carpeta de red compartida, puede configurarla para que utilice políticas estándar de control de aplicaciones o bien puede crear políticas personalizadas de control de aplicaciones. Si desea que una aplicación BlackBerry Java Application utilice políticas de control de aplicaciones personalizadas, debe crearlas antes de agregar la aplicación a una configuración de software. Al agregar la aplicación a una configuración de software, puede seleccionar qué política personalizada de control de aplicaciones desea aplicar a la aplicación.

Si agrega la aplicación BlackBerry Java Application a varias configuraciones de software y también asigna a BlackBerry Java Application distintas políticas personalizadas de control de aplicaciones en las distintas configuraciones de software, debe configurar la prioridad de las políticas personalizadas de control de aplicaciones. Esta prioridad determina qué política personalizada de control de aplicaciones aplica BlackBerry Policy Service si asigna varias configuraciones de software a una cuenta de usuario.

1. En la barra de menús, haga clic en **Configuración de BlackBerry OS**.

2. Haga clic en **Administrar aplicaciones**.
3. Busque una aplicación BlackBerry Java Application.
4. En los resultados de búsqueda, haga clic en una aplicación BlackBerry Java Application.
5. En la sección **Versiones de las aplicaciones**, haga clic en la versión de la aplicación para la que desea crear una política personalizada de control de aplicaciones.
6. Haga clic en **Editar aplicación**.
7. En la pestaña **Políticas de control de aplicaciones**, en la sección **Configuración**, seleccione la opción **Usar políticas de control de aplicaciones personalizadas**.
8. Lleve a cabo cualquiera de las tareas siguientes:

Tarea	Pasos
Crear una política de control de aplicaciones para aplicaciones BlackBerry Java Applications necesarias.	a. En el campo **Nombre de la aplicación obligatoria**, escriba un nombre para la política de control de aplicaciones. b. En la sección **Configuración**, configure los ajustes de la política de control de aplicaciones. c. Haga clic en el icono **Agregar**. d. Repita los pasos de la "a" a la "c" por cada política de control de aplicaciones que desee crear.
Crear una política de control de aplicaciones para aplicaciones opcionales BlackBerry Java Applica	a. En el campo **Nombre de aplicación opcional**, escriba un nombre para la política de control de aplicaciones. b. En la sección **Configuración**, configure los ajustes de la política de control de aplicaciones. c. Haga clic en el icono **Agregar**. d. Repita los pasos del 1 al 3 por cada política de control de aplicaciones que desee crear.
Crear una política de control de aplicaciones para aplicaciones BlackBerry Java Applications que no estén permitidas.	a. En el campo **Nombre de aplicación no permitida**, escriba un nombre para la política de control de aplicaciones. b. Haga clic en el icono **Agregar**.

9. Si fuera necesario, en cada sección, haga clic en las flechas arriba y abajo para establecer la prioridad de las políticas de control de aplicaciones.
10. Haga clic en **Guardar todo**.

Clasificación de las reglas de políticas de TI en los dispositivos con BlackBerry OS

La configuración de la regla de política de TI anula la configuración de la regla de política de control de aplicaciones. Por ejemplo, si cambia la regla de política de TI Permitir las conexiones internas a No para los dispositivos con BlackBerry OS (de la versión 5.0 a la 7.1) y si estos dispositivos tienen un conjunto de políticas de control de aplicaciones que permite a una aplicación específica realizar conexiones internas, la aplicación no podrá realizar conexiones internas.

El dispositivo revoca una política de control de aplicaciones y se restablece si los permisos de la aplicación a la que se aplican pasan a ser más restrictivos. Los dispositivos permiten que los usuarios establezcan permisos de aplicaciones más restrictivos, pero nunca menos restrictivos, que los especificados por usted.

Políticas de control de aplicaciones para las aplicaciones que no figuran en la lista

Cuando se crea una configuración de software y se asigna a cuentas de usuario para poder enviar la configuración de BlackBerry Device Software, de las aplicaciones BlackBerry Java Applications y de aplicaciones estándar a dispositivos con BlackBerry OS (de la versión 5.0 a la 7.1), debe especificar si la configuración de software permite a los usuarios instalar y utilizar aplicaciones que no están incluidas en la configuración de software (también conocidas como aplicaciones que no figuran en la lista). Cuando se configura si las aplicaciones que no aparecen en la lista están permitidas y son opcionales, o no están permitidas en los dispositivos con BlackBerry OS, se debe asignar una política de control de aplicaciones para las aplicaciones que no figuran en la lista a la configuración de software.

Una política de control de aplicaciones para las aplicaciones que no figuran en la lista determina cuales de las aplicaciones que no aparecen en la lista están permitidas en los dispositivos con BlackBerry OS y cuáles son los datos a los que pueden acceder las aplicaciones que no aparecen en la lista en los dispositivos con BlackBerry OS. Existen dos políticas de control de aplicaciones estándar para aplicaciones que no figuran en la lista: una para las que son opcionales y otra para las que no están permitidas. Puede cambiar la configuración predeterminada de la política estándar de control de aplicaciones para las aplicaciones no que no figuran en la lista que son opcionales o bien puede crear políticas personalizadas de control de aplicaciones para dichas aplicaciones.

Cambio de la política estándar de control de aplicaciones para las aplicaciones que no figuran en la lista que son opcionales

1. En la barra de menús, haga clic en **Configuración de BlackBerry OS**.
2. Amplíe **Software**.
3. Haga clic en **Gestionar políticas de control de aplicaciones para aplicaciones que no figuran en la lista**.
4. Haga clic en la política de control de aplicaciones **Opcionales estándar que no figuran en la lista**.
5. Haga clic en **Editar política de control de aplicaciones**.
6. En la pestaña **Configuración de acceso**, en la sección **Configuración**, configure los ajustes de la política de control de aplicaciones.
7. Haga clic en **Guardar todo**.

Crear una política de control de aplicaciones para aplicaciones que no figuran en la lista

Existen dos políticas de control de aplicaciones predeterminadas para las aplicaciones que no aparecen en la lista: una para las aplicaciones que no aparecen en la lista, pero que se autorizan en los dispositivos con BlackBerry OS (de la versión 5.0 a la 7.1) y otra para las aplicaciones que no aparecen en la lista, pero que no se autorizan en los dispositivos con BlackBerry OS. También puede crear políticas personalizadas de control de aplicaciones para aplicaciones que no aparecen en la lista que son opcionales.

1. En la barra de menús, haga clic en **Configuración de BlackBerry OS**.
2. Amplíe **Software**.
3. Haga clic en **Crear una política de control de aplicaciones para aplicaciones que no figuran en la lista**.
4. En la sección **Información de la política de control de aplicaciones**, en el campo **Nombre**, escriba un nombre para la política de control de aplicaciones para las aplicaciones que no figuren en la lista.
5. Haga clic en **Guardar**.
6. En el menú **Administración de la solución BlackBerry**, haga clic en **Gestionar políticas de control de aplicaciones para aplicaciones que no figuran en la lista**.
7. Haga clic en la política de control de aplicaciones que ha creado.
8. Haga clic en **Editar política de control de aplicaciones**.
9. En la pestaña **Configuración de acceso**, en la sección **Configuración**, configure los ajustes de la política de control de aplicaciones.

10. Haga clic en **Guardar todo**.

Configuración de la prioridad de las políticas de control de aplicaciones para las aplicaciones que no figuran en la lista

Puede asignar varias configuraciones de software a las cuentas de usuario. Puede asignar diferentes políticas de control de aplicaciones para aplicaciones que no aparecen en la lista a diferentes configuraciones de software. Debe configurar la prioridad de las diferentes políticas de control de aplicaciones para aplicaciones que no aparecen en la lista de modo que BlackBerry Policy Service pueda determinar qué políticas de control de aplicaciones aplicar a cuentas de usuario cuando asigne varias configuraciones de software a cuentas de usuario.

1. En la barra de menús, haga clic en **Configuración de BlackBerry OS**.
2. Amplíe **Software**.
3. Haga clic en **Gestionar políticas de control de aplicaciones para aplicaciones que no figuran en la lista**.
4. Haga clic en **Establecer la prioridad de las políticas de control de aplicaciones para las aplicaciones que no figuran en la lista**.
5. Haga clic en las flechas arriba y abajo para establecer la prioridad de las políticas de control de aplicaciones para aplicaciones que no figuran en la lista.
6. Haga clic en **Guardar**.

Creación de configuraciones de software

Puede utilizar las configuraciones de software para realizar las acciones siguientes en dispositivos con BlackBerry OS (de la versión 5.0 a la 7.1):

- Asignar políticas de control de acceso a aplicaciones BlackBerry Java Applications para controlar los permisos de aplicaciones y los datos a los pueden obtener acceso las aplicaciones
- Especificar que una aplicación BlackBerry Java Application no está permitida
- Especificar si las aplicaciones BlackBerry Java Applications que no ha incluido en la configuración de software se admiten o no se admiten
- Configurar los permisos de acceso para las aplicaciones BlackBerry Java Applications que no ha incluido en la configuración de software
- Instalar o actualizar BlackBerry Device Software a través de la red inalámbrica o mediante BlackBerry Web Desktop Manager
- Especificar la configuración de aplicaciones estándar

Pasos para crear y asignar una configuración de software

Al crear y asignar una configuración de software, debe realizar las acciones siguientes:

Paso	Acción
1	Cree y comparta una carpeta de red.
2	Agregue las aplicaciones.
3	Si es necesario, cree una política de control de aplicaciones personalizadas.

Paso	Acción
4	Cree una configuración de software.
5	Agregue el software a la configuración de software.
6	Asigne la configuración de software a una cuenta de usuario o a un grupo de usuarios.

Crear una configuración de software

1. En la barra de menús, haga clic en **Configuración de BlackBerry OS**.
2. Amplíe **Software**.
3. Haga clic en **Crear una configuración de software**.
4. En la sección **Información de la configuración**, en el campo **Nombre**, escriba un nombre para la configuración de software.
5. En la lista desplegable **Disposición para las aplicaciones que no figuran en la lista**, lleve a cabo una de las acciones siguientes:
   - Para permitir que los usuarios instalen aplicaciones que no están incluidas en la configuración de software de sus dispositivos con BlackBerry OS, haga clic en **Opcional**.
   - Para impedir que los usuarios instalen aplicaciones que no están incluidas en la configuración de software de sus dispositivos con BlackBerry OS, haga clic en **No permitido**.
6. En la lista desplegable **Política de control de aplicaciones para aplicaciones que no figuran en la lista**, haga clic en la política de control de aplicaciones para las aplicaciones que no figuran en la lista que desea asignar a la configuración de software.
7. Haga clic en **Guardar**.

Después de terminar: Agregue las configuraciones de BlackBerry Device Software y las aplicaciones BlackBerry Java Applications a la configuración de software.

Adición de una BlackBerry Java Application a una configuración de software

Para instalar la aplicación BlackBerry Java Application en los dispositivos con BlackBerry OS (de la versión 5.0 a la 7.1) a través de la red inalámbrica, es necesario agregar la aplicación BlackBerry Java Application a una configuración de software y asignar dicha configuración a las cuentas de usuario. Para actualizar una aplicación, debe agregar la nueva versión de la aplicación a la configuración de software correspondiente. BlackBerry UEM actualiza la aplicación presente en los dispositivos con BlackBerry OS con la nueva versión.

1. En la barra de menús, haga clic en **Configuración de BlackBerry OS**.
2. Amplíe **Software**.
3. Haga clic en **Administrar configuraciones de software**.
4. Haga clic en la configuración de software a la que desea agregar una aplicación BlackBerry Java Application.
5. Haga clic en **Editar configuración de software**.
6. En la pestaña **Aplicaciones**, haga clic en **Agregar aplicaciones a una configuración de software**.
7. Busque las aplicaciones BlackBerry Java Applications que desea agregar a la configuración de software.

8. En los resultados de búsqueda, seleccione una aplicación BlackBerry Java Application que desee agregar a la configuración de software.
9. En la lista desplegable **Disposición** de la aplicación BlackBerry Java Application, realice una de las acciones siguientes:
   - Para instalar la aplicación BlackBerry Java Application automáticamente en los dispositivos con BlackBerry OS e impedir que los usuarios la eliminen, haga clic en **Obligatoria**.
   - Para permitir a los usuarios instalar y eliminar la aplicación BlackBerry Java Application, haga clic en **Opcional**.
   - Para impedir que los usuarios instalen una aplicación BlackBerry Java Application en los dispositivos con BlackBerry OS, haga clic en **No permitido**.
10. En la sección **Datos de la aplicación** y en la lista desplegable **Política de control de aplicaciones**, haga clic en la política de control de aplicaciones que va a aplicar a la aplicación BlackBerry Java Application.
11. Si es necesario, en la lista desplegable **Implementación**, lleve a cabo una de las acciones siguientes:
   - Para instalar la aplicación en los dispositivos con BlackBerry OS a través de la red inalámbrica, haga clic en **Inalámbrico**.
   - Para instalar la aplicación en dispositivos con BlackBerry OS por medio de una conexión USB con el equipo del usuario y BlackBerry Web Desktop Manager, haga clic en **Con cable**.
12. Repita los pasos 6 a 10 para cada aplicación BlackBerry Java Application que desee agregar a la configuración de software.
13. Haga clic en **Agregar a la configuración de software**.
14. Haga clic en **Guardar todo**.

Instalación de aplicaciones BlackBerry Java Applications en un dispositivo con BlackBerry OS en un equipo central

Si no desea instalar aplicaciones BlackBerry Java Applications en un dispositivo con BlackBerry OS (de la versión 5.0 a la 7.1) a través de la red inalámbrica y no desea que el usuario instale aplicaciones BlackBerry Java Applications mediante BlackBerry Web Desktop Manager o BlackBerry Desktop Software, puede instalar aplicaciones BlackBerry Java Applications en un dispositivo con BlackBerry OS conectando el dispositivo BlackBerry a un equipo central que pueda obtener acceso a BlackBerry UEM.

Antes de empezar:

- Asigne una configuración de software con las aplicaciones BlackBerry Java Applications necesarias a la cuenta de usuario apropiada.
- Para permitir que la consola de gestión conecte con un dispositivo con BlackBerry OS que está vinculado con el equipo que aloja la consola de gestión de BlackBerry UEM a través de una conexión USB, agregue la dirección web de la consola de gestión a la lista de sitios web de confianza en el navegador web. Vuelva a iniciar sesión en la consola de gestión.
- Compruebe que el equipo central pueda acceder a la consola de gestión.
- Conecte el dispositivo con BlackBerry OS que está asociado a la cuenta de usuario del equipo central.

1. En la barra de menús, haga clic en **Configuración de BlackBerry OS**.
2. Amplíe **Dispositivos conectados**.
3. Haga clic en **Software del dispositivo**.
4. Haga clic en **Instalación automática de aplicaciones en el dispositivo BlackBerry**.
5. Siga las instrucciones que aparecen en pantalla.

Presentación de los usuarios que tienen una aplicación BlackBerry Java Application instalada en sus dispositivos con BlackBerry OS

1. En la barra de menús, haga clic en **Configuración de BlackBerry OS**.
2. Amplíe **Software > Aplicaciones**.
3. Haga clic en **Administrar aplicaciones**.
4. Busque una aplicación.
5. En los resultados de la búsqueda, haga clic en el nombre de una aplicación.
6. En la sección **Versiones de las aplicaciones**, haga clic en una versión de la aplicación.
7. Haga clic en **Ver usuarios con la aplicación**.
8. Busque los usuarios que están asociados a los dispositivos con BlackBerry OS en los que ha instalado la aplicación BlackBerry Java Application.

Reglas de reconciliación para conflictos de ajustes en las configuraciones de software

Si asigna varias configuraciones de software a cuentas de usuario o grupos de usuarios, las distintas configuraciones de software pueden contener conflictos de ajustes. Por ejemplo, puede especificar que una aplicación BlackBerry Java Application es necesaria en una configuración de software que asigna a una cuenta de usuario, pero también puede especificar que la misma aplicación no está permitida en una configuración de software que asigne a un grupo de usuarios al que pertenece la cuenta de usuario. Pueden generarse conflictos al asignar varias aplicaciones BlackBerry Java Applications, políticas de control de aplicaciones, políticas de control de aplicaciones para aplicaciones no listadas, BlackBerry Device Software y las opciones de aplicación estándar en las configuraciones de BlackBerry Device Software.

BlackBerry UEM utiliza reglas de reconciliación predefinidas para resolver conflictos de ajustes entre varias configuraciones de software y para determinar qué aplicaciones, software y configuración se han instalado o aplicado en un dispositivo con BlackBerry OS (de la versión 5.0 a 7.1). BlackBerry UEM resuelve los conflictos de ajustes como una actividad asincrónica en segundo plano. Puede ver el resultado de las actividades de reconciliación, los errores de reconciliación y las aplicaciones, el software y la configuración que BlackBerry UEM ha aplicado a un dispositivo con BlackBerry OS.

BlackBerry UEM puede tener que reconciliar los ajustes de configuración de software en conflicto si realiza cualquiera de las siguientes acciones:

- Activar un dispositivo
- Asignar un nuevo dispositivo con BlackBerry OS o PIN a un usuario
- Agregar una cuenta de usuario o eliminarla de un grupo
- Agregar un grupo o eliminarlo de otro grupo
- Agregar una aplicación o eliminarla de una configuración de software
- Cambiar la configuración de una aplicación en una configuración de software
- Cambiar la configuración de una política de control de aplicaciones
- Cambiar la clasificación de las políticas de control de aplicaciones
- Instalar una versión nueva de BlackBerry Device Software en un dispositivo con BlackBerry OS
- Agregar una configuración de BlackBerry Device Software a una configuración de software o eliminar una configuración de BlackBerry Device Software de una configuración de software
- Cambiar una configuración de BlackBerry Device Software
- Cambiar la configuración de aplicaciones estándar en una configuración de BlackBerry Device Software

Reglas de reconciliación: BlackBerry Java Applications

Situación	Regla
Varias configuraciones de software se asignan a una cuenta de usuario o a los grupos a los que pertenece el usuario. En cada configuración de software se incluyen varias aplicaciones BlackBerry Java Applications.	Las aplicaciones BlackBerry Java Applications de cada configuración de software están instaladas en el dispositivo con BlackBerry OS (de la versión 5.0 a la 7.1). Si BlackBerry Device Software no admite una determinada aplicación BlackBerry Java Application, esta no se instala en el dispositivo con BlackBerry OS.
Varias configuraciones de software que contienen diferentes versiones de la misma aplicación BlackBerry Java Application se asignan a una cuenta de usuario o a los grupos a los que pertenece dicho usuario.	Cuando existen versiones diferentes de una aplicación en las configuraciones de software que se han asignado a una cuenta de usuario, la versión más reciente admitida por BlackBerry Device Software se instala en el dispositivo con BlackBerry OS. Por ejemplo, si una configuración de software con la versión 1.0 de una aplicación se ha asignado a una cuenta de usuario y otra configuración de software con la versión 2.0 de la aplicación se ha asignado a una cuenta de usuario, la versión 2.0 de la aplicación se instala en el dispositivo con BlackBerry OS. La versión de una aplicación BlackBerry Java Application que está en una configuración de software que se ha asignado a una cuenta de usuario tiene prioridad sobre la versión de una aplicación BlackBerry Java Application que está en una configuración de software que se ha asignado a un grupo. Por ejemplo, si la versión 1.0 de una aplicación está en una configuración de software que se ha asignado a una cuenta de usuario y la versión 2.0 de una aplicación está en una configuración de software que se ha asignado a un grupo al que pertenece el usuario, la versión 1.0 de la aplicación se instala en el dispositivo con BlackBerry OS.

Situación	Regla
Varias configuraciones de software que contienen la misma aplicación BlackBerry Java Application se asignan a una cuenta de usuario o a los grupos a los que pertenece el usuario. La disposición de la aplicación BlackBerry Java Application (obligatoria, opcional o no permitida) es diferente en cada configuración de software. El método de implementación (con cable o a través de la red inalámbrica) para la aplicación es distinta en cada configuración de software.	La disposición especificada para una aplicación en una configuración de software que se ha asignado a una cuenta de usuario tiene prioridad sobre la disposición de la misma aplicación en cualquier configuración de software que se ha asignado a un grupo. Si la aplicación tiene disposiciones diferentes en varias configuraciones de software que están asignadas en el mismo nivel (cuenta de usuario o grupos), la disposición obligatoria tiene prioridad sobre la disposición opcional y la disposición opcional tiene prioridad sobre la disposición no permitida. BlackBerry UEM resuelve el método de implementación después de resolver la disposición de una aplicación. El método de implementación especificado para una aplicación en una configuración de software que se asigna a una cuenta de usuario tiene prioridad sobre el método de implementación para la misma aplicación en cualquier configuración de software que se asigna a un grupo. La configuración inalámbrica tiene prioridad sobre la configuración de red con cable.
Una o más configuraciones de software que incluyen aplicaciones BlackBerry Java Applications se asignan a una cuenta de usuario o a los grupos a los que pertenece el usuario, pero en el dispositivo con BlackBerry OS queda una cantidad limitada de memoria disponible.	BlackBerry UEM comprueba la cantidad de memoria disponible en el dispositivo con BlackBerry OS después de resolver los conflictos de aplicaciones (por ejemplo, tras resolver los conflictos de ajustes de disposición y de implementación) y antes de instalar una aplicación BlackBerry Java Application. Si no hay suficiente memoria disponible en el dispositivo con BlackBerry OS para admitir la aplicación, esta no se instala. Dependiendo de la cantidad de memoria disponible, las aplicaciones se instalan en el siguiente orden: **1.** Las aplicaciones obligatorias que están configuradas para la implementación inalámbrica **2.** Las aplicaciones obligatorias que están configuradas para la implementación con cable **3.** Las aplicaciones opcionales que están configuradas para la implementación inalámbrica **4.** Las aplicaciones opcionales que están configuradas para la implementación con cable

Situación	Regla
Una configuración de software se asigna a una cuenta de usuario y contiene una aplicación BlackBerry Java Application que tiene una dependencia con respecto a otra aplicación BlackBerry Java Application.	Si una aplicación BlackBerry Java Application de una configuración de software depende de otra aplicación y esa aplicación no está incluida en una configuración de software asignada a la cuenta de usuario o a un grupo al que pertenece el usuario, la aplicación no se instala en el dispositivo con BlackBerry OS. Si una aplicación BlackBerry Java Application de una configuración de software depende de otra aplicación y la aplicación dependiente está incluida en una configuración de software asignada a la cuenta de usuario o a un grupo al que pertenece el usuario, la aplicación dependiente se instala en primer lugar. Si la aplicación dependiente se instala correctamente, la aplicación con la dependencia se instala a continuación.
Una configuración de software se asigna a una cuenta de usuario y contiene una aplicación BlackBerry Java Application que tiene una dependencia con respecto a otra aplicación BlackBerry Java Application. La aplicación dependiente no se admite en el dispositivo con BlackBerry OS.	Si una aplicación dependiente no se admite en el dispositivo con BlackBerry OS ni se ha instalado correctamente en el dispositivo con BlackBerry OS, la aplicación con la dependencia no se instala en el dispositivo con BlackBerry OS del usuario.
Varias aplicaciones BlackBerry Java Applications tienen una dependencia circular (por ejemplo, la aplicación A depende de la aplicación B, la aplicación B depende de la aplicación C y la aplicación C depende la aplicación A) y están incluidas en el mismo paquete de aplicaciones. El paquete de aplicaciones se agrega al repositorio de aplicaciones. Las aplicaciones se agregan a una configuración de software y se asignan a una cuenta de usuario o a un grupo al que pertenece el usuario.	Si se incluyen varias aplicaciones BlackBerry Java Applications en el mismo paquete de aplicaciones y tienen una dependencia circular, las aplicaciones no se instalan en el dispositivo con BlackBerry OS. Si varias aplicaciones tienen una dependencia circular, solo se pueden instalar si existen en paquetes de aplicaciones independientes y se instalan mediante la implementación con cable.

Reglas de reconciliación: BlackBerry Device Software

Situación	Regla
Una configuración de software que contiene BlackBerry Device Software se asigna a una cuenta de usuario. Una configuración de software que contiene una versión diferente de BlackBerry Device Software se asigna a un grupo al que pertenece la cuenta de usuario.	El BlackBerry Device Software en una configuración de software que se asigna a una cuenta de usuario tiene prioridad sobre el BlackBerry Device Software en una configuración de software que se asigna a un grupo.

Situación	Regla
Varias configuraciones de software que contienen diferentes versiones de BlackBerry Device Software se asignan a una cuenta de usuario.	La versión de BlackBerry Device Software que es compatible con el dispositivo con BlackBerry OS (de la versión 5.0 a la 7.1) y con el proveedor de servicios inalámbricos, y que, además, tiene la clasificación más alta en la consola de gestión de BlackBerry UEM, se instala en el dispositivo con BlackBerry OS. BlackBerry UEM no instala una versión de BlackBerry Device Software si esa versión tiene una clasificación inferior a la versión de BlackBerry Device Software que está instalada actualmente en el dispositivo BlackBerry OS.

Reglas de reconciliación: la configuración de aplicación estándar

Situación	Regla
Una configuración de software con configuración de aplicación estándar se asigna a una cuenta de usuario. Una configuración de software con diferentes configuraciones de aplicación estándar se asigna a un grupo al que pertenece la cuenta de usuario.	La configuración de aplicación estándar en una configuración de software que se asigna a una cuenta de usuario tiene prioridad sobre la configuración de aplicación estándar en una configuración de software que se asigna a un grupo.
Una cuenta de usuario pertenece a varios grupos. La configuración de la vista inicial del calendario está configurada de forma diferente en cada una de las configuraciones de software que se han asignado a los grupos.	La configuración de la vista inicial del calendario que se aplica al usuario del dispositivo con BlackBerry OS (de la versión 5.0 a la 7.1) es el valor más bajo que se ha especificado en las diferentes configuraciones de software.
Una cuenta de usuario pertenece a varios grupos. La configuración del recordatorio de las citas del calendario está configurada de forma diferente en cada una de las configuraciones de software que se han asignado a los grupos.	La configuración del recordatorio de las citas del calendario que se aplica al usuario del dispositivo con BlackBerry OS es el valor más alto que se ha especificado en las diferentes configuraciones de software.
Una cuenta de usuario pertenece a varios grupos. La configuración de correo para confirmar la eliminación de mensajes se establece en Sí en una o más de las configuraciones de software que se han asignado a los grupos. La configuración se establece en No en el resto de configuraciones de software.	Si la configuración de correo para confirmar la eliminación de mensajes se establece en Sí en una configuración de software que está asignada a un grupo al que pertenece la cuenta de usuario, la configuración Sí se aplica al dispositivo con BlackBerry OS.
Una cuenta de usuario pertenece a varios grupos. La configuración de correo para ocultar los mensajes enviados se establece en Sí en una o más de las configuraciones de software que se han asignado a los grupos. La configuración se establece en No en el resto de configuraciones de software.	Si la configuración de correo para ocultar los mensajes enviados se establece en Sí en una configuración de software que está asignada a un grupo al que pertenece la cuenta de usuario, la configuración No se aplica al dispositivo con BlackBerry OS.

Situación	Regla
Una cuenta de usuario pertenece a varios grupos. La configuración de correo para guardar una copia en la bandeja de enviados se establece en Sí en una o más de las configuraciones de software que se han asignado a los grupos. La configuración se establece en No en el resto de configuraciones de software.	Si la configuración de correo para guardar una copia en la bandeja de enviados se establece en Sí en una configuración de software que está asignada a un grupo al que pertenece la cuenta de usuario, la configuración Sí se aplica al dispositivo con BlackBerry OS.
Una cuenta de usuario pertenece a varios grupos. La configuración del orden de la libreta de direcciones está configurada de forma diferente en cada una de las configuraciones de software que se han asignado a los grupos.	La configuración del orden de la libreta de direcciones está configurada de forma diferente en cada una de las configuraciones de software que se han asignado a los grupos a los que pertenece la cuenta de usuario: la configuración del nombre tiene prioridad sobre la de los apellidos, y la de los apellidos sobre la del nombre de la empresa.
Una cuenta de usuario pertenece a varios grupos. La configuración de atributos para las distintas configuraciones de aplicaciones estándar está configurada de forma distinta en las configuraciones de software que se han asignado a los grupos.	La configuración de bloqueado y visible tiene prioridad sobre la de desbloqueado y visible. La configuración de desbloqueado y visible tiene prioridad sobre la de desbloqueado y oculto.
La configuración de aplicación estándar está establecida en una configuración de software y asignada a las cuentas de usuario con dispositivos con BlackBerry OS que ejecutan una versión de BlackBerry Device Software anterior a la versión 5.0.	La configuración de aplicación estándar solo se aplica a los dispositivos con BlackBerry OS que ejecutan BlackBerry Device Software versión 5.0 o posterior.

Reglas de reconciliación: políticas de control de aplicaciones

Situación	Regla
A un usuario se le asignan varias configuraciones de software que contienen la misma aplicación. Una política de control de aplicaciones distinta se asigna a la aplicación en cada configuración de software.	Una política de control de aplicaciones para una aplicación en una configuración de software que se asigna a una cuenta de usuario tiene prioridad sobre la política de control de aplicación para la misma aplicación en una configuración de software que se asigna a un grupo. La configuración Obligatorio tiene prioridad sobre la configuración Opcional. La configuración Opcional tiene prioridad sobre la configuración No permitido. Si varias configuraciones de software contienen la misma aplicación y a cada configuración de software se le asigna una política de control de aplicaciones personalizada diferente con la misma disposición (por ejemplo, dos políticas de control de aplicaciones necesarias personalizadas), la política de control de aplicaciones que tiene la clasificación más alta en la consola de gestión de BlackBerry UEM se aplica al dispositivo con BlackBerry OS (de la versión 5.0 a la 7.1) del usuario.

Reglas de reconciliación: políticas de control de las aplicaciones para las aplicaciones que no figuran en la lista

Situación	Regla
Una configuración de software con una política de control de aplicaciones para las aplicaciones que no figuran en la lista, ya sea predeterminada o personalizada, se asigna a una cuenta de usuario. Una configuración de software con una política de control de aplicaciones para las aplicaciones que no figuran en la lista distinta se asigna a un grupo al que pertenece la cuenta de usuario.	La política de control de aplicaciones para las aplicaciones que no figuran en la lista en una configuración de software que se asigna a una cuenta de usuario tiene prioridad sobre la política de control de aplicaciones para las aplicaciones que no figuran en una configuración de software que se asigna a un grupo.
Una configuración de software que define aplicaciones que no figuran en la lista como no permitidas se asigna a una cuenta de usuario. Una configuración de software que define aplicaciones que no figuran en la lista como opcional se asigna también a la cuenta de usuario.	Si las aplicaciones que no constan en la lista se definen como no permitidas en una configuración de software que está asignada a una cuenta de usuario, las aplicaciones no listadas no estarán permitidas en el dispositivo con BlackBerry OS (de la versión 5.0 a la 7.1).
Varias configuraciones de software con distintas políticas de control de aplicaciones para aplicaciones no listadas se asignan a una cuenta de usuario.	La política de control de aplicaciones para las aplicaciones que no figuran en la lista con la clasificación más alta en la consola de gestión de BlackBerry UEM se aplica al dispositivo con BlackBerry OS.

Usuarios y grupos

Puede crear cuentas de usuario y, a continuación, crear grupos de usuarios para gestionar los usuarios y los dispositivos de manera eficiente.

Pasos para crear grupos y cuentas de usuario

Al administrar los usuarios y dispositivos de la empresa, debe realizar las acciones siguientes:

Paso	Acción
1	Cree funciones de usuario.
2	Cree grupos de usuarios.
3	Cree cuentas de usuario.
4	Opcionalmente, cree grupos de dispositivos.

Creación de funciones de usuario

Las funciones de usuario le permiten especificar las capacidades que están disponibles para los usuarios en BlackBerry UEM Self-Service.

BlackBerry UEM Incluye una función de usuario predeterminada preconfigurada. La función de usuario predeterminada está configurada para permitir todas las capacidades de BlackBerry UEM Self-Service, y se ha asignado al grupo "Todos los usuarios". Puede editar las capacidades de la función de usuario predeterminada.

Nota: Al renombrar, eliminar o quitar la función de usuario predeterminada el grupo "Todos los usuarios", se pueden producir problemas con la aplicación Aplicaciones de trabajo en dispositivos iOS.

Si desea restringir determinadas capacidades de BlackBerry UEM Self-Service para los usuarios, puede crear nuevas funciones de usuario o editar una función de usuario existente. Puede asignar funciones de usuario a grupos o directamente a usuarios.

Capacidades de BlackBerry UEM Self-Service

La siguiente tabla enumera las capacidades de BlackBerry UEM Self-Service:

Capacidad	Descripción
Especificar una contraseña de activación	Esta capacidad permite a los usuarios crear contraseñas de activación que pueden utilizar para activar sus dispositivos en BlackBerry UEM. Puede configurar el período de caducidad y la complejidad de la contraseña predeterminada en Configuración > Autoservicio > Configuración de autoservicio.

Capacidad	Descripción
Especificar clave de acceso	Esta capacidad permite a los usuarios crear claves de acceso que pueden utilizar para activar aplicaciones BlackBerry Dynamics.
Eliminar solo los datos de trabajo	Esta capacidad permite a los usuarios enviar el comando "Eliminar solo datos de trabajo" a un dispositivo. El comando elimina los datos de trabajo, incluidos la política de TI, los perfiles, las aplicaciones y los certificados.
Eliminar todos los datos del dispositivo	Esta capacidad permite a los usuarios enviar el comando "Eliminar todos los datos del dispositivo" a un dispositivo. El comando elimina toda la información del usuario y los datos de las aplicaciones que guarda el dispositivo, incluida la información del espacio de trabajo. Devuelve el dispositivo a los valores predeterminados de fábrica y elimina el dispositivo de BlackBerry UEM.
Ubicar dispositivo	Esta capacidad permite a los usuarios ver la ubicación de sus dispositivos iOS, Android o Windows 10 Mobile en un mapa. Esta capacidad requiere que un perfil de servicio de ubicación esté asignado al usuario. Para obtener más información, consulte Creación de un perfil de servicio de ubicación.
Administrar certificados de usuario	Esta función permite a los usuarios cargar certificados de usuario para sus dispositivos. Puede proporcionar instrucciones a los usuarios acerca de los certificados que necesitan y desde dónde cargar dichos certificados.
Bloqueo y desbloqueo de aplicaciones BlackBerry Dynamics	Si los dispositivos de usuario están habilitados para BlackBerry Dynamics, esta capacidad permite a los usuarios bloquear las aplicaciones de BlackBerry Dynamics instaladas en sus dispositivos y generar claves de desbloqueo para desbloquear las aplicaciones. Cuando un usuario bloquea una aplicación, nadie podrá abrirla.
Eliminar datos de aplicaciones BlackBerry Dynamics	Si los dispositivos de usuario están habilitados para BlackBerry Dynamics, esta capacidad permite a los usuarios eliminar todos los datos de una aplicación BlackBerry Dynamics instalada en un dispositivo. El comando elimina todos los datos almacenados por la aplicación, pero la aplicación no se elimina.

Cree una función de usuario

Puede crear una función de usuario personalizada y asignarla a usuarios o grupos para especificar las capacidades que los usuarios tienen en BlackBerry UEM Self-Service.

1. En la barra de menú, haga clic en **Configuración > Autoservicio**.
2. Haga clic en **Funciones de usuarios**.
3. Haga clic en .
4. Escriba un nombre y una descripción para la función de usuario.
5. Para copiar permisos de otra función, haga clic en una función de la lista desplegable **Permisos copiados de la función**.
6. Seleccione las capacidades que desea que tenga un usuario.
7. Haga clic en **Guardar**.

Cómo elige BlackBerry UEM qué función de usuario asignar

Solo se asigna una función a un usuario. BlackBerry UEM utiliza las reglas siguientes para determinar qué función asignar a un usuario:

- Una función asignada directamente a una cuenta de usuario tiene prioridad sobre una función asignada indirectamente por grupo de usuarios.
- Si un usuario es miembro de varios grupos de usuarios que tienen funciones de usuario diferentes, BlackBerry UEM asigna la función con la clasificación más alta.

Clasifique las funciones de usuario

La clasificación se usa para determinar qué función asigna BlackBerry UEM a un usuario cuando son miembros de varios grupos de usuarios con funciones diferentes.

1. En la barra de menú, haga clic en **Configuración > Autoservicio**.
2. Haga clic en **Funciones de usuarios**.
3. Utilice las flechas para mover las funciones hacia arriba o hacia abajo en la clasificación.
4. Haga clic en **Guardar**.

Asigne una función de usuario a un grupo

Una función de usuario especifica las capacidades disponibles para los usuarios en BlackBerry UEM Self-Service.

Antes de empezar: Cree una función de usuario.

1. En la barra de menú, haga clic en **Grupos**.
2. Busque un grupo de usuarios.
3. En los resultados de la búsqueda, haga clic en el nombre del grupo de usuarios.
4. Haga clic en la pestaña **Dispositivos gestionados**.
5. En la sección **Función de usuario**, haga clic en +.
6. En la lista desplegable, haga clic en el nombre de la función que desea asignar al grupo.
7. Haga clic en **Agregar** o **Sustituir**.

Asigne una función de usuario a un usuario

Una función de usuario especifica las capacidades disponibles para los usuarios en BlackBerry UEM Self-Service.

Antes de empezar: Cree una función de usuario.

1. En la barra de menú, haga clic en **Users**.
2. Seleccione la pestaña **Todos los usuarios** o **Dispositivos gestionados**.
3. Busque una cuenta de usuario.
4. En los resultados de la búsqueda, haga clic en el nombre de la cuenta de usuario.
5. Haga clic en ✎.
6. En la lista desplegable **Asignación directa de funciones**, seleccione la función que desea asignar. Si selecciona **Ninguno**, un grupo asignará la función del usuario. Si no hay ninguna asignación de grupo, el usuario no tendrá acceso a BlackBerry UEM Self-Service.
7. Haga clic en **Guardar**.

Creación y administración de cuentas de usuario

Puede agregar cuentas de usuario directamente a BlackBerry UEM, o si se ha conectado BlackBerry UEM al directorio de la empresa, puede agregar cuentas de usuario desde el directorio de la empresa. Para obtener más información acerca de la conexión de BlackBerry UEM a un directorio de la empresa y de la activación de grupos vinculados a directorios, consulte el contenido referente a Configuración.

También puede utilizar un archivo .csv para agregar varias cuentas de usuario de BlackBerry UEM al mismo tiempo.

Creación de una cuenta de usuario

Antes de empezar:

- Si desea agregar un usuario de directorio, compruebe que BlackBerry UEM esté conectado al directorio de la empresa. Para obtener más información acerca de la conexión de BlackBerry UEM a un directorio de la empresa y de la activación de grupos vinculados a directorios, consulte el contenido referente a Configuración.
- Si desea habilitar el servicio BlackBerry Workspaces para sus usuarios, verifique que el complemento de Workspaces para BlackBerry UEM está instalado en cada instancia de BlackBerry UEM de su entorno. Para obtener más información sobre la instalación del servicio Workspaces, póngase en contacto con su representante de la cuenta de Workspaces.

1. En la barra de menú, haga clic en **Usuarios > Dispositivos gestionados**.
2. Haga clic en **Agregar usuario**.
3. Lleve a cabo una de las tareas siguientes:

Tarea	Pasos
Adición de un usuario de directorio	**a.** En la pestaña **Directorio de la empresa**, en el campo de búsqueda, especifique los criterios de búsqueda para el usuario de directorio que desea agregar. Puede buscar por nombre, apellidos, nombre para mostrar, nombre de usuario o dirección de correo. **b.** En los resultados de la búsqueda, seleccione la cuenta de usuario.
Adición de un usuario local	**a.** Haga clic en la pestaña **Local**. **b.** Escriba el **Nombre** y los **Apellidos** de la cuenta de usuario. **c.** En el campo **Nombre para mostrar**, realice los cambios que sean necesarios. El nombre para mostrar se configura automáticamente con el nombre y los apellidos que se han especificado. **d.** En el campo **Nombre de usuario**, introduzca un nombre de usuario exclusivo para la cuenta de usuario. **e.** En el campo **Dirección de correo**, introduzca una dirección de correo de contacto para la cuenta de usuario. Se necesita una dirección de correo electrónico para la cuenta de usuario a fin de activar un servicio como, por ejemplo, Workspaces o la administración de dispositivos. **f.** También puede hacer clic en **Detalles adicionales del usuario** y rellenar los campos según corresponda.

4. Si existen grupos locales en BlackBerry UEM y desea agregar la cuenta de usuario a grupos, en la lista **Grupos disponibles**, seleccione uno o más grupos y haga clic en ➡.

Al crear una cuenta de usuario, puede agregarla únicamente a grupos locales en BlackBerry UEM. Si la cuenta de usuario es miembro de un grupo vinculado a directorios, automáticamente se asocia con dicho grupo cuando se produce la sincronización entre BlackBerry UEM y el directorio de la empresa.

Para agregar una cuenta de usuario a los grupos a los que se le asignó una función administrativa, debe ser un Administrador de seguridad.

5. Si agrega un usuario local, cree una contraseña para BlackBerry UEM Self-Service en el campo **Contraseña de la cuenta**. Si el usuario tiene asignada una función administrativa, también pueden usar la contraseña para acceder a la consola de gestión.
6. En la sección **Servicios activados**, seleccione la opción **Activar usuario para la administración de dispositivos**.
7. Si el complemento Workspaces para BlackBerry UEM está instalado en el dominio, para activar el servicio Workspaces, realice las siguientes acciones:
   a) En la sección **BlackBerry Workspaces**, seleccione la casilla de verificación **Activar BlackBerry Workspaces**. De forma predeterminada, los usuarios con el servicio Workspaces reciben la función de Visitante.
   b) Seleccione una o más funciones de usuario. Haga clic en ➡.
8. Lleve a cabo una de las tareas siguientes:

Tarea	Pasos
Pedir a los usuarios que activen los dispositivos con el perfil de activación actualmente asignado.	**a.** En la lista desplegable **Opción de activación**, seleccione **Activación del dispositivo predeterminada**. **b.** En la lista desplegable **Contraseña de activación**, seleccione si desea configurar la contraseña o generar automáticamente una contraseña. **c.** De manera opcional, puede cambiar la caducidad del periodo de activación. La caducidad del periodo de activación especifica cuánto tiempo la contraseña de activación sigue siendo válida. **d.** Si desea que la contraseña de activación sea válida solo para una activación de dispositivo, seleccione **El periodo de activación caduca después de la activación del primer dispositivo**. **e.** En la lista desplegable **Plantilla del correo de activación**, seleccione la plantilla que desea utilizar para el correo de activación.
Empareje una contraseña de activación con un perfil de activación específico.	**a.** En la lista desplegable **Opción de activación**, seleccione **Activación del dispositivo con perfil de activación especificado**. **b.** En la lista desplegable **Perfil de activación**, seleccione el perfil de activación que desee emparejar con una contraseña. **c.** En la lista desplegable **Contraseña de activación**, seleccione si desea configurar la contraseña o generar automáticamente una contraseña. **d.** De manera opcional, puede cambiar la caducidad del periodo de activación. La caducidad del periodo de activación especifica cuánto tiempo la contraseña de activación sigue siendo válida. **e.** Si desea que la contraseña de activación sea válida solo para una activación de dispositivo, seleccione **El periodo de activación caduca después de la activación del primer dispositivo**. **f.** En la lista desplegable **Plantilla del correo de activación**, haga clic en la plantilla que desea utilizar para correo de activación.

Tarea	Pasos
Permitir a los usuarios activar solo aplicaciones de BlackBerry Dynamics.	**a.** En la lista desplegable **Opción de activación**, seleccione **Generación de clave de acceso de BlackBerry Dynamics**. **b.** En la lista desplegable **Número de claves de acceso que se van a generar**, seleccione el número de claves. Cada clave solo puede usarse una vez para activar una aplicación de BlackBerry Dynamics. **c.** Seleccione el número de días que desea que la clave de acceso siga siendo válida. **d.** En la lista desplegable **Plantilla del correo de activación**, haga clic en la plantilla que desea utilizar para correo de activación.
Agregar usuario a BlackBerry UEM solamente.	**a.** En la lista desplegable **Opción de activación**, seleccione **No establecer**.

9. Si el dominio de BlackBerry UEM admite los dispositivos con BlackBerry OS (la versión 5.0 a la 7.1), para activar la activación del dispositivo con BlackBerry OS para un usuario de directorio, realice las acciones siguientes:
   a) Seleccione la casilla de verificación **Permitir que el usuario active un dispositivo con BlackBerry OS**.
   b) En la lista desplegable **Servidor de correo de BlackBerry OS**, haga clic en el nombre de un servidor.

   Nota: El directorio de usuario debe existir en el servidor de correo de trabajo con el que se conecta el servidor de correo de BlackBerry OS.
10. Si utiliza variables personalizadas, amplíe **Variables personalizadas** y especifique los valores apropiados para las variables que se han definido.
11. Lleve a cabo una de las siguientes acciones:
    - Para guardar la cuenta de usuario, haga clic en **Guardar**.
    - Para guardar la cuenta de usuario y crear otra, haga clic en **Guardar y crear nueva**.

Conceptos relacionados

Permitir que los usuarios activen varios dispositivos con diferentes tipos de activación
Plantillas de correo

Referencia relacionada

Variables personalizadas

Creación de cuentas de usuario desde un archivo .csv

Puede crear el archivo .csv manualmente mediante el archivo .csv de muestra de BlackBerry UEM, que se puede descargar desde la pestaña Importar en la ventana Agregar un usuario.

Acerca de las cuentas de usuario en archivos .csv

Puede importar cuentas de usuario en un archivo .csv a BlackBerry UEM para crear muchas cuentas de usuario a la vez. En función de sus necesidades, también puede especificar la pertenencia al grupo y los ajustes de activación de las cuentas de usuario al incluir las siguientes columnas en el archivo .csv:

Encabezado de columna	Descripción
Suscripción de grupo	Asigne uno o más grupos de usuarios a cada cuenta de usuario. Utilice un punto y coma (;) para separar varios grupos de usuarios. Si no se incluye la columna "Suscripción de grupo", al importar el archivo, se le dará la opción de seleccionar el grupo al que desea que se agreguen todas las cuentas de usuario importadas. Si desea asignar a cada cuenta de usuario a un grupo de usuarios específico, utilice esta columna antes de importar el archivo.
MDM (BlackBerry UEM)	Especifique si el usuario está activado para MDM. Para activar un usuario para MDM, escriba "Activado".
Contraseña de activación	Introduzca la contraseña de activación. Este valor es necesario si el valor "Generación de la contraseña de activación" se establece en "manual".
Plantilla de activación	Introduzca el nombre de la plantilla de correo de activación que desea enviar al usuario. Si no especifica un nombre, se utiliza la plantilla de correo de activación predeterminada.
Caducidad de la contraseña de activación	Introduzca el número de segundos que la contraseña de activación es válida antes de que caduque.
Generación de la contraseña de activación	Introduzca una de las siguientes opciones: • Automático. La contraseña de activación se crea automáticamente y se envía al usuario. • Manual. La contraseña de activación se establece en la columna "Contraseña de activación". Si el valor se deja en blanco, el valor predeterminado es Automático.
Enviar correo electrónico de activación	Introduzca una de las siguientes opciones: • Verdadero. El correo de activación se envía al usuario. • Falso. El correo de activación no se envía al usuario. Si la "Generación de la contraseña de activación" se establece en "Automático", el correo de activación se envía al usuario independientemente del valor en esta columna. Si el valor "Generación de la contraseña de activación" es "Manual" y está vacío, el valor predeterminado será Verdadero.
Tipo de usuario	Esta columna es obligatoria siempre que el archivo .csv incluya tanto cuentas de usuario locales como de directorio. Introduzca una de las siguientes opciones: • L para cuentas de usuario locales • D para cuentas de usuario de directorio Las entradas no distinguen entre mayúsculas y minúsculas.

Encabezado de columna	Descripción
UID del directorio	(Opcional) Una alternativa a la inserción de la dirección de correo para las cuentas de usuario de directorio. De forma predeterminada, la dirección de correo se usa para validar las cuentas de usuario de directorio; sin embargo, puede especificar que el directorio UID se utilice en su lugar. Si la cuenta de usuario no se puede validar en el directorio UID, se informa de un error. Si incluye un valor de UID del directorio para uno de sus usuarios, el encabezado de columna debe incluir el UID del directorio y todas las filas del archivo .csv deben incluir un UID del directorio o tener un marcador de posición vacío (,) para la columna UID del directorio.

Para ver un ejemplo del archivo .csv, haga clic en **Usuarios > Todos los usuarios > Agregar usuario > Importar > Descargar archivo de muestra .csv**.

¿Cómo valida BlackBerry UEM el archivo .csv de cuentas de usuario?

BlackBerry UEM valida el archivo .csv de cuentas de usuario antes, durante e inmediatamente después de que se cargue el archivo .csv e informa de los errores que encuentre.

Los siguientes son algunos de los errores que impedirán que BlackBerry UEM cargue el archivo .csv:

- Un formato de archivo o una extensión no válida
- Un archivo sin datos
- El número de columnas no coincide con el número de encabezados del archivo

Cuando BlackBerry UEM encuentra un error, detiene la carga del archivo y muestra un mensaje de error. Se debe corregir el error y, a continuación, volver a cargar el archivo .csv.

Después de que el archivo .csv se cargue, BlackBerry UEM muestra una lista de las cuentas de usuario que serán importadas y, si procede, cualquier cuenta de usuario de directorio que no se importará como resultado de un error (por ejemplo, una entrada duplicada o dirección de correo no válida). Puede realizar una de las acciones siguientes:

- Cancelar la operación, corregir los errores y, a continuación, volver a cargar el archivo .csv.
- Continuar y cargar las cuentas de usuario válidas. Las cuentas de usuario de directorio con errores no se cargan. Debe copiar y corregir las cuentas de usuario de directorio que no se cargan en un archivo .csv independiente. De lo contrario, volver a cargar el mismo archivo .csv dará como resultado errores de duplicación para las cuentas de usuario que se han cargado correctamente.

BlackBerry UEM realiza una validación final de las cuentas de usuario importadas justo antes de crear las cuentas de usuario para asegurarse de que no haya errores como resultado del proceso de importación del archivo (por ejemplo, otro administrador creó una cuenta de usuario solo como un archivo .csv que contenía la misma cuenta de usuario que se estaba importado).

Adición de cuentas de usuario mediante un archivo .csv

Para ver un ejemplo de un archivo .csv, consulte Acerca de las cuentas de usuario en archivos .csv.

Antes de empezar:

- Si el archivo .csv contiene cuentas de usuario de directorio, compruebe que BlackBerry UEM esté conectado al directorio de la empresa.

- Verifique que el número de columnas coinciden con el número de encabezados en el archivo .csv.
- Compruebe que se incluyan las columnas requeridas.
- Compruebe que la información de las columnas sea correcta.

1. En la barra de menú, haga clic en **Usuarios**.
2. Seleccione la pestaña **Todos los usuarios** o **Dispositivos gestionados**.
3. Haga clic en **Agregar usuario**.
4. Haga clic en la pestaña **Importar**.
5. Haga clic en **Examinar** y desplácese hasta el archivo .csv que contiene las cuentas de usuario que desea agregar.
6. Haga clic en **Cargar**.
7. Si se informa de errores, realice las siguientes acciones:
   a) Corrija los errores en el archivo .csv.
   b) Haga clic en **Examinar** y navegue hasta el archivo .csv.
   c) Haga clic en **Cargar**.
   d) Repita el paso 6 hasta que todos los errores se hayan corregido.
8. Si el archivo .csv no utiliza la columna "Suscripción de grupo" y los grupos locales se encuentran en BlackBerry UEM, realice las siguientes acciones si desea agregar cuentas de usuario a los grupos:
   a) En la lista **Grupos disponibles**, seleccione uno o más grupos y haga clic en ➡.
   b) Haga clic en **Siguiente**.

   Al importar el archivo .csv, todas las cuentas de usuario se agregan a los grupos locales que se seleccionan. Si una cuenta de usuario es miembro de un grupo vinculado a directorios, automáticamente se asocia a dicho grupo cuando se produce la sincronización entre BlackBerry UEM y el directorio la empresa.

   Para agregar cuentas de usuario a grupos a los que se les asignó una función administrativa, debe ser un administrador de seguridad.
9. Revise la lista de cuentas de usuario y realice una de las siguientes acciones:
   - Para corregir los errores de cualquier cuentas de usuario de directorio no validas, haga clic en **Cancelar** y diríjase al paso 6.
   - Para agregar las cuentas de usuario válidas, haga clic en **Importar**. Cualquiera de las cuentas de usuario de directorio no válidas se ignoran.

Después de terminar: Si el dominio de BlackBerry UEM admite los dispositivos con BlackBerry OS (de la versión 5.0 a la 7.1), para activar la activación del dispositivo con BlackBerry OS para cuentas de usuario de directorio, edite la información de la cuenta de usuario.

Tareas relacionadas

Edición de la información de la cuenta de usuario

Consulta de una cuenta de usuario

Puede ver la información de una cuenta de usuario en la pestaña Resumen. Por ejemplo, puede ver la información siguiente:

- Dispositivos activados
- Grupos de usuarios a los que pertenece una cuenta de usuario
- Asignación de la política de TI, de perfiles y de aplicaciones

1. En la barra de menú, haga clic en **Users**.
2. Busque una cuenta de usuario mediante una de las opciones siguientes:

- Haga clic en **Todos los usuarios**, y escriba en el campo **Buscar**.
- Haga clic en **Dispositivos gestionados > Búsqueda de usuario** y escriba en el campo de búsqueda.

3. En los resultados de la búsqueda, haga clic en el nombre de la cuenta de usuario.

Adición de notas a una cuenta de usuario

Puede agregar notas a fin de efectuar el seguimiento de información relacionada con una cuenta de usuario específica. La información de la nota se almacena junto con la cuenta de usuario y no con un dispositivo individual. Si el usuario se elimina, la información en el campo notas también se elimina. El uso de la función de notas está controlado por el permiso "Editar usuarios" para los administradores.

1. En la barra de menú, haga clic en **Users**.
2. Busque una cuenta de usuario.
3. En los resultados de la búsqueda, haga clic en el nombre de una cuenta de usuario.
4. Haga clic en el icono **Agregar nota** en la esquina superior derecha.
5. Introduzca las notas en el cuadro de diálogo que se abre. Las notas que escriba se guardarán automáticamente y el icono cambiará para indicar que hay notas guardadas.

Gestione varias cuentas de usuario al mismo tiempo

Puede completar determinadas acciones para varios usuarios al mismo tiempo. Por ejemplo, puede enviar un correo electrónico a un grupo de usuarios seleccionado.

Antes de empezar: Establezca la vista predeterminada o avanzada.

1. En la barra de menú, haga clic en **Usuarios > Dispositivos gestionados**.
2. Si es necesario, Filtrado de la lista de usuarios.
3. Lleve a cabo una de las siguientes acciones:
   - Seleccione la casilla de verificación en la parte superior de la lista de usuarios para seleccionar todos los usuarios.
   - Seleccione la casilla de verificación de cada usuario que desee incluir en el archivo. Puede utilizar Mayús +clic para seleccionar varios usuarios.
4. En el menú, haga clic en uno de los siguientes iconos:

Icono	Descripción
	Envío de un correo a los usuarios
	Envío de un mensaje de correo electrónico de activación a varios usuarios
	Agregar usuarios a los grupos de usuarios
	Exportación de la lista de usuarios a un archivo .csv
	Enviar una contraseña de BlackBerry UEM Self-Service a varios usuarios

Envío de un correo a los usuarios

Se puede enviar un correo a uno o a más usuarios directamente desde la consola de gestión. Los usuarios deben tener una dirección de correo asociada a su cuenta.

El correo se envía desde la dirección de correo que haya configurado en la configuración del servidor SMTP.

Antes de empezar: Para enviar un correo electrónico a varios usuarios, se debe asignar una función administrativa que tenga el permiso "Enviar correo a usuarios".

1. En la barra de menú, haga clic en **Users**.
2. Seleccione la pestaña **Todos los usuarios** o **Dispositivos gestionados**.
3. Lleve a cabo una de las tareas siguientes:

Tarea	Pasos
Envío de un correo a un usuario	**a.** Busque una cuenta de usuario. **b.** En los resultados de la búsqueda, haga clic en el nombre de la cuenta de usuario. **c.** Haga clic en . **d.** Opcionalmente, haga clic en **CC** e introduzca una o más direcciones de correo (separadas por comas o por puntos y comas) para copiar el mensaje de correo a sí mismo o a otros.
Envío de un correo a varios usuarios	**a.** Seleccione la casilla de verificación para cada usuario al que desee enviar un correo. **b.** Haga clic en . **c.** Opcionalmente, haga clic en **Para** o **CC** e introduzca una o más direcciones de correo (separadas por comas o por puntos y comas) para enviar o copiar el mensaje de correo a sí mismo o a otros.

4. Escriba un asunto y un mensaje.
5. Haga clic en **Enviar**.

Enviar una contraseña de BlackBerry UEM Self-Service a varios usuarios

Puede enviar una contraseña de UEM Self-Service a varios usuarios al mismo tiempo. Las contraseñas se generan aleatoriamente y se envía un mensaje de correo que contiene las contraseñas a los usuarios.

El correo se envía desde la dirección de correo que haya configurado en la configuración del servidor SMTP.

1. En la barra de menú, haga clic en **Usuarios > Dispositivos gestionados**.
2. Seleccione los usuarios a los que desea enviar la contraseña de UEM Self-Service. Tenga en cuenta que los usuarios deben tener una dirección de correo asociada a su cuenta.
3. Haga clic en .
4. Haga clic en **Continuar**.

Edición de la información de la cuenta de usuario

Puede editar la siguiente información de usuario:

- Nombre, nombre de usuario, nombre de visualización y dirección de correo electrónico
- Permanencia a grupo (no se ha podido cambiar la pertenencia a los grupos vinculados a directorios).
- Contraseña de la cuenta para cuentas de usuario local
- Función de usuario
- Si ha definido variables personalizadas, puede editar la información variable

- Si el dominio BlackBerry UEM es compatible con los dispositivos con BlackBerry OS (de la versión 5.0 a la 7.1), puede activar o desactivar la activación del dispositivo con BlackBerry OS para las cuentas de usuario del directorio. Puede desactivar la activación del dispositivo con BlackBerry OS solo si el usuario no ha activado un dispositivo con BlackBerry OS.

Nota: No se pueden editar los detalles del usuario administrador predeterminado ni de los usuarios que utilizan las credenciales de su cuenta de BlackBerry Online.

1. En la barra de menú, haga clic en **Usuarios > Dispositivos gestionados**.
2. Busque una cuenta de usuario.
3. En los resultados de la búsqueda, haga clic en el nombre de la cuenta de usuario.
4. Haga clic en .
5. Edite la información de la cuenta de usuario.
6. Haga clic en **Guardar**.

Sincronización de la información del usuario del directorio

Si ha agregado una cuenta de usuario desde el directorio de la empresa, puede sincronizar manualmente la información de dicho usuario con el directorio de la empresa en cualquier momento, en lugar de esperar la hora de sincronización automática.

1. En la barra de menú, haga clic en **Users**.
2. Seleccione la pestaña **Todos los usuarios** o **Dispositivos gestionados**.
3. Busque una cuenta de usuario.
4. En los resultados de la búsqueda, haga clic en el nombre de la cuenta de usuario.
5. Haga clic en .

Cambio de la sincronización de datos del organizador y la configuración de correo para un usuario de dispositivo con BlackBerry OS

En la Configuración avanzada en la pestaña Resumen, puede cambiar los ajustes de sincronización de datos del organizador para una cuenta de usuario. También puede administrar el reenvío de mensajes, controlar qué carpetas puede sincronizar un usuario con un dispositivo con BlackBerry OS y administrar firmas y renuncias en mensajes de correo.

1. En la barra de menú, haga clic en **Usuarios**.
2. Busque una cuenta de usuario.
3. En los resultados de la búsqueda, haga clic en el nombre de la cuenta de usuario.
4. En la sección **Política de TI, perfiles y configuraciones de software**, haga clic en **Configuración avanzada**.
5. Haga clic en **Editar usuario**.
6. En la sección **Configuración de la mensajería**, haga clic en **Configuración predeterminada**.
7. Haga los cambios en las pestañas apropiadas.
8. Haga clic en **Continuar a la edición de la información del usuario**.
9. Haga clic en **Guardar todo**.

Elimine los servicios de un usuario

Si se ha activado BlackBerry UEM para uno o más servicios de valor añadido, y se activa a un usuario para un servicio, puede eliminar el servicio del usuario. También puede eliminar los controles MDM, sin eliminar la cuenta de usuario de BlackBerry UEM.

Antes de empezar:

- Antes de poder eliminar los controles MDM, debe eliminar los dispositivos activados de un usuario.
- Antes de poder eliminar el servicio de Enterprise Identity, debe eliminar todas las asignaciones de Enterprise Identity.

1. En la barra de menú, haga clic en **Usuarios > Todos los usuarios**.
2. Busque una cuenta de usuario.
3. En los resultados de la búsqueda, haga clic en el nombre de la cuenta de usuario.
4. Haga clic en ⛔.
5. Lleve a cabo cualquiera de las tareas siguientes:

Tarea	Pasos
Eliminar servicios MDM	**a.** Haga clic en ⛔ en Dispositivos gestionados. **b.** Haga clic en **Guardar**.
Eliminar servicio Workspaces	**a.** Haga clic en ⛔ en Workspaces. **b.** En la pantalla de diálogo **Eliminar WatchDox by BlackBerry**, seleccione una de las opciones siguientes: • Eliminar todos los archivos propiedad de este usuario y revocar la pertenencia a todos los grupos y las listas de distribución del espacio de trabajo • Transferir los archivos de este usuario y su suscripción a los grupos y las listas de distribución del espacio de trabajo a una dirección de correo diferente. En el campo **Dirección de correo**, escriba una dirección de correo de contacto. Se crea una nueva cuenta de usuario si la dirección de correo no está asociada a una cuenta de usuario existente. **c.** Haga clic en **Eliminar**.
Eliminar servicio Enterprise Identity	**a.** Haga clic en ⛔ en Enterprise Identity. **b.** Haga clic en **Guardar**.

Después de terminar: Para activar un servicio, consulte Active los servicios de un usuario.

Active los servicios de un usuario

Si se ha activado BlackBerry UEM para uno o más servicios de valor añadido, puede activar un servicio para un usuario.

1. En la barra de menú, haga clic en **Usuarios > Todos los usuarios**.
2. Busque una cuenta de usuario.
3. En los resultados de la búsqueda, haga clic en el nombre de la cuenta de usuario.
4. Lleve a cabo cualquiera de las tareas siguientes:

Tarea	Pasos
Activar servicios MDM	**a.** Haga clic en + en Dispositivos gestionados. **b.** Si existen grupos locales en BlackBerry UEM y desea agregar la cuenta de usuario a grupos, en la lista **Grupos disponibles**, seleccione uno o más grupos y haga clic en →. **c.** Elija una opción para la contraseña de activación del dispositivo. **d.** Haga clic en **Guardar**.
Activar el servicio Workspaces	**a.** Haga clic en + en Workspaces. **b.** Asigne funciones de Workspaces. **c.** Haga clic en **Guardar**.
Activar el servicio Enterprise Identity	**a.** Haga clic en + en Enterprise Identity. **b.** Seleccione los grupos de aplicaciones **c.** Haga clic en **Asignar**.

Eliminar una cuenta de usuario

Cuando se elimina una cuenta de usuario, los datos de trabajo también se eliminan de todos los dispositivos del usuario.

Antes de empezar:

- Desactive cualquier dispositivo asociado a la cuenta de usuario que desea eliminar.
- Elimine cualquier servicio asociado a la cuenta de usuario que desea eliminar. Para obtener más información, consulte Elimine los servicios de un usuario.

1. En la barra de menú, haga clic en **Usuarios > Dispositivos gestionados**.
2. Busque una cuenta de usuario.
3. En los resultados de la búsqueda, seleccione el nombre de una cuenta de usuario.
4. Haga clic en 🗑.
5. Haga clic en **Eliminar**.

Conceptos relacionados

Desactivación de dispositivos

Agregar usuarios a los grupos de usuarios

Nota: Para agregar un usuario al que se le asigna una función administrativa a un grupo de usuarios, debe ser un administrador de seguridad.

1. En la barra de menú, haga clic en **Usuarios > Dispositivos gestionados**.
2. Seleccione la casilla de verificación junto a los usuarios que desea agregar a los grupos de usuarios.
3. Haga clic en 👥.
4. En la lista **Grupos disponibles**, seleccione uno o más grupos y haga clic en →.

   Nota: No se ha podido cambiar la pertenencia a los grupos vinculados a directorios.
5. Haga clic en **Guardar**.

Eliminación de un usuario de un grupo de usuarios

No se puede eliminar un usuario desde un grupo vinculado a directorios.

Nota: Para eliminar un usuario que tiene asignada una función administrativa de un grupo de usuarios, debe ser un administrador de seguridad.

1. En la barra de menús, haga clic en **Grupos**.
2. Busque el grupo de usuarios que desea editar.
3. Haga clic en el grupo de usuarios.
4. Busque el usuario que desea eliminar.
5. Seleccione el usuario.
6. Haga clic en .

Cambio de los grupos de usuarios a los que pertenece un usuario

Nota: Para cambiar a qué grupos de usuarios pertenece un usuario que tiene asignada una función administrativa, debe ser un administrador de seguridad.

1. En la barra de menú, haga clic en **Usuarios > Dispositivos gestionados**.
2. Busque una cuenta de usuario.
3. En los resultados de la búsqueda, haga clic en el nombre de la cuenta de usuario.
4. En la sección **Suscripción de grupo**, haga clic en .
5. Realice cualquiera de las tareas siguientes:
   - Para agregar un usuario a los grupos de usuarios, en la lista **Grupos disponibles**, seleccione uno o más grupos y haga clic en .
   - Para eliminar el usuario de los grupos de usuarios, en la lista **Miembro de grupos**, seleccione uno o más grupos y haga clic en .

   Nota: No se ha podido cambiar la pertenencia a los grupos vinculados a directorios.
6. Haga clic en **Guardar**.

Asignar un perfil o una política de TI a una cuenta de usuario

1. En la barra de menú, haga clic en **Usuarios > Dispositivos gestionados**.
2. Busque una cuenta de usuario.
3. En los resultados de la búsqueda, haga clic en el nombre de la cuenta de usuario.
4. En la sección **Política de TI y perfiles**, haga clic en .
5. Haga clic en **Política de TI** o en un tipo de perfil.
6. En la lista desplegable, haga clic en el nombre del perfil o la política de TI que desea asignar al usuario.
7. Para las políticas de TI y la clasificación de los tipos de perfil, si el tipo de perfil que ha seleccionado en el paso 5 ya está asignado directamente al usuario, haga clic en **Sustituir**. De lo contrario, haga clic en **Asignar**.

Conceptos relacionados

¿Cómo elige BlackBerry UEM qué política de TI asignar?
Asignación de perfiles
¿Cómo elige BlackBerry UEM qué perfiles asignar?

Tareas relacionadas

Creación de una política de TI
Crear un perfil de requisitos de solicitud de servicio del dispositivo para dispositivos con BlackBerry 10
Asignación de un perfil o una política de TI a un grupo de usuarios

Adición de un certificado de cliente a una cuenta de usuario

Puede agregar un certificado de cliente a una cuenta de usuario individual y enviar el certificado a dispositivos con BlackBerry Dynamics u otros dispositivos gestionados iOS y Android.

Agregue certificados de cliente a cuentas de usuario cuando los dispositivos de usuarios necesiten certificados para S/MIME o autenticación de cliente y el certificado no se pueda enviar a los dispositivos a través de un perfil de credenciales de usuario o perfil SCEP.

El certificado de cliente debe tener una extensión de nombre de archivo .pfx o p12. Puede enviar más de un certificado de cliente a los dispositivos.

También puede utilizar los perfiles de credenciales de usuario para cargar certificados para usuarios individuales. Los perfiles de credenciales de usuario se pueden asociar a un perfil de Wi-Fi, VPN o correo.

1. En la barra de menú, haga clic en **Usuarios > Dispositivos gestionados**.
2. Busque una cuenta de usuario.
3. En los resultados de la búsqueda, haga clic en el nombre de una cuenta de usuario.
4. En la sección **Política de TI y perfiles**, haga clic en +.
5. Haga clic en **Certificado de usuario**.
6. Escriba una descripción para el certificado.
7. En la sección **Aplicar certificado a**, seleccione una de las opciones siguientes:
   - **Otros dispositivos gestionados**: seleccione esta opción para enviar el certificado a dispositivos iOS y Android para todos los usos admitidos excepto para aplicaciones de BlackBerry Dynamics.
   - **Dispositivos con BlackBerry Dynamics**: seleccione esta opción para enviar el certificado a dispositivos para utilizarlo con aplicaciones de BlackBerry Dynamics.
8. En el campo **Archivo de certificado**, haga clic en **Examinar** para ubicar el archivo de certificado.
9. Si ha seleccionado **Otros dispositivos administrados**, en el campo **Contraseña**, escriba una contraseña para el certificado. Para dispositivos de iOS, se requiere una contraseña. Para dispositivos de Android, no es necesario proporcionar una contraseña en BlackBerry UEM si el dispositivo dispone de la última versión de BlackBerry UEM Client. Si no establece una contraseña, el usuario debe introducir la contraseña del dispositivo.
10. Haga clic en **Agregar**.
    El certificado se incluye en la tabla **Certificados de usuario** de la página de resumen de usuario.

Después de terminar:

- Para dispositivos con BlackBerry Dynamics, configure el periodo de tiempo en que los certificados cargados permanecen en el BlackBerry UEM servidor antes de que se eliminen automáticamente de este. La configuración predeterminada es 24 horas.

Conceptos relacionados

Envío de certificados a dispositivos mediante perfiles

Cambie un certificado de cliente por una cuenta de usuario

1. En la barra de menú, haga clic en **Usuarios > Dispositivos gestionados**.
2. Busque una cuenta de usuario.
3. En los resultados de la búsqueda, haga clic en el nombre de una cuenta de usuario.
4. En la sección **Política de TI y perfiles**, haga clic en el certificado de usuario que desea cambiar.
5. Haga clic en .
6. Realice los cambios necesarios. No puede cambiar los dispositivos a los que se aplica el certificado.
7. Haga clic en **Guardar**.

Después de terminar: Si cambia un certificado de usuario de BlackBerry Dynamics que usted o un usuario han eliminado de un dispositivo, el certificado se volverá a enviar al dispositivo.

Renovación o eliminación de un certificado de BlackBerry Dynamics para una cuenta de usuario

Puede enviar un comando al dispositivo de un usuario para solicitar la renovación del certificado de la entidad de certificación. También puede eliminar un certificado de BlackBerry Dynamics del dispositivo de un usuario. Si elimina un certificado, el conector de PKI de BlackBerry Dynamics envía una notificación a la entidad de certificación de que el certificado ya no está en uso, aunque el certificado no se revoca automáticamente.

1. En la barra de menú, haga clic en **Usuarios > Dispositivos gestionados**.
2. Busque una cuenta de usuario.
3. En los resultados de la búsqueda, haga clic en el nombre de una cuenta de usuario.
4. En la sección **Certificados de usuario**, realice una de las siguientes acciones:
   - Haga clic en para solicitar la renovación del certificado de la entidad de certificación.
   - Haga clic en para eliminar el certificado de los dispositivos del usuario.

   Nota: Para eliminar una credencial inteligente de Entrust de un dispositivo, el usuario también debe desactivar la credencial inteligente en BlackBerry UEM Client.

Tareas relacionadas

Renovación de certificados que están escritos mediante el conector de PKI de BlackBerry Dynamics

Adición de un certificado de cliente a un perfil de credenciales de usuario

Puede cargar certificados para usuarios individuales a un perfil de credenciales de usuario. Los usuarios también pueden cargar su certificado al perfil de credenciales de usuario mediante BlackBerry UEM Self-Service. Se admite la carga de certificados en los perfiles de credenciales de usuario para dispositivos con BlackBerry 10 OS versión 10.3.1 y posteriores, dispositivos iOS y dispositivos Android con un espacio de trabajo.

El certificado de cliente debe tener una extensión de nombre de archivo .pfx o p12. Si se carga un certificado nuevo al perfil de credenciales de usuario, se sustituye el certificado existente en los dispositivos de usuario.

Antes de empezar:

- Cree un perfil de credenciales de usuario para cargar manualmente los certificados.
- Asigne el perfil de credenciales de usuario a los usuarios.

1. En la barra de menú, haga clic en **Usuarios > Dispositivos gestionados**.
2. Busque una cuenta de usuario.
3. En los resultados de la búsqueda, haga clic en el nombre de una cuenta de usuario.

4. En la sección **Política de TI y perfiles**, junto al perfil de credenciales de usuario, haga clic en **Agregar certificado**.
5. Haga clic en **Examinar** para buscar el archivo de certificado.
6. Introduzca la contraseña del certificado. Para dispositivos iOS, se requiere la contraseña. Para dispositivos Android, no es necesario proporcionar la contraseña en BlackBerry UEM si el dispositivo dispone de la última versión de BlackBerry UEM Client. Si no especifica la contraseña, el usuario debe introducir la contraseña del dispositivo.
7. Haga clic en **Agregar**.

Tareas relacionadas

Cree un perfil de credenciales de usuario para cargar manualmente los certificados

Cambie un certificado de cliente por un perfil de credenciales de usuario

Puede cambiar el certificado que usted o un usuario han añadido a un perfil de credenciales de usuario. El nuevo certificado sustituye el certificado existente en el dispositivo.

1. En la barra de menú, haga clic en **Usuarios > Dispositivos gestionados**.
2. Busque una cuenta de usuario.
3. En los resultados de la búsqueda, haga clic en el nombre de una cuenta de usuario.
4. En la sección **Política de TI y perfiles**, en la fila del perfil de credenciales de usuario, haga clic en **Actualizar**.
5. Haga clic en **Examinar** para buscar el archivo de certificado.
6. Escriba una contraseña para el certificado. Para dispositivos de iOS, se requiere una contraseña. Para dispositivos Android, no es necesario proporcionar la contraseña en BlackBerry UEM si el dispositivo dispone de la última versión de BlackBerry UEM Client. Si no especifica la contraseña, el usuario debe introducir la contraseña del dispositivo.
7. Haga clic en **Guardar**.

Tareas relacionadas

Cree un perfil de credenciales de usuario para cargar manualmente los certificados

Asignación de una aplicación a una cuenta de usuario

Si necesita controlar las aplicaciones en el nivel de usuario, puede asignar aplicaciones o grupos de aplicaciones a cuentas de usuario. Cuando se asigna una aplicación a un usuario, la aplicación está disponible para cualquier dispositivo que el usuario haya activado para ese tipo de dispositivo y la aplicación aparece en el catálogo de aplicaciones de trabajo en el dispositivo.

También puede asignar aplicaciones a los usuarios para tipos de dispositivo que el usuario no haya activado todavía. Si el usuario activa un tipo de dispositivo diferente en el futuro, las aplicaciones adecuadas estarán disponibles para el dispositivo nuevo del usuario.

La misma aplicación puede asignarse directamente a la cuenta de usuario o puede heredarse de grupos de usuarios o de dispositivos. La configuración de la aplicación (por ejemplo, si la aplicación es obligatoria) se asigna en función de la prioridad: los grupos de dispositivos tienen la prioridad más alta, a continuación, las cuentas de usuario y, por último, los grupos de usuarios.

Antes de empezar:

- Adición de la aplicación a la lista de aplicaciones disponibles
- Opcionalmente, adición de las aplicaciones a un grupo de aplicaciones

1. En la barra de menú, haga clic en **Usuarios > Dispositivos gestionados**.
2. Busque una cuenta de usuario.
3. En los resultados de la búsqueda, haga clic en el nombre de una cuenta de usuario.
4. En la sección **Aplicaciones**, haga clic en +.
5. Seleccione la casilla de verificación junto a las aplicaciones o el grupo de aplicaciones que desea asignar a la cuenta del usuario.
6. Haga clic en **Siguiente**.
7. En la lista desplegable **Disposición** de la aplicación, realice una de las acciones siguientes:
   - Para obligar a los usuarios a instalar la aplicación, seleccione **Obligatorio**.
   - Para permitir a los usuarios instalar y eliminar la aplicación, seleccione **Opcional**.

   Nota: Si la misma aplicación se asigna a una cuenta de usuario, un grupo de usuarios al que pertenece el usuario y el grupo de dispositivos al que pertenece el dispositivo, tiene prioridad la disposición de la aplicación asignada al grupo de dispositivos.
8. En los dispositivos iOS, para asignar los ajustes de VPN por aplicación a una aplicación o grupo de aplicaciones, en la lista desplegable **VPN por aplicación** para la aplicación o grupo de aplicaciones, seleccione los ajustes que desea asociar a la aplicación o grupo de aplicaciones.
9. Para dispositivos iOS y Android, si hay disponible una configuración de aplicaciones, seleccione la configuración de aplicaciones que desee asignar a la aplicación.
10. Si agrega una aplicación iOS, realice una de las tareas siguientes:

Tarea	Pasos
Si no ha agregado una cuenta de VPP o no va a agregar una aplicación iOS	**a.** Haga clic en **Asignar**.
Si va a agregar una aplicación iOS y ha agregado al menos una cuenta de VPP	**a.** Haga clic en **Siguiente**. **b.** Seleccione **Sí** si desea asignar una licencia a la aplicación iOS. Seleccione **No** si no desea asignar una licencia o no tiene una licencia que asignar a la aplicación. **c.** Si ha asignado una licencia a la aplicación, en la lista desplegable **Licencia de la aplicación**, seleccione la cuenta de VPP para asociarla a la aplicación. **d.** En la lista desplegable **Asignar licencia a**, asigne la licencia al **Usuario** o al **Dispositivo**. Si no se especifica el valor en la lista desplegable **Licencia de la aplicación**, la lista desplegable **Asignar licencia a** no está disponible. **e.** Haga clic en **Asignar**. Los usuarios deben seguir las instrucciones para inscribirse en el programa de compras por volumen (VPP) en los dispositivos de la empresa antes de poder instalar aplicaciones de prepago. Los usuarios deben completar esta tarea una vez. **Nota:** Si concede acceso a un número de licencias superior al número de licencias disponibles, los primeros usuarios que accedan a las licencias disponibles podrán instalar la aplicación. Si la aplicación es una aplicación obligatoria que no tiene una licencia disponible, debe obtener la licencia antes de que el usuario pueda instalar la aplicación o dicho usuario estará sujeto a las reglas de cumplimiento que se hayan asignado al usuario.

Referencia relacionada

Comportamiento de la aplicación en los dispositivos Android
Comportamiento de la aplicación en los dispositivos iOS
Comportamiento de la aplicación en los dispositivos BlackBerry

Asignación de un grupo de aplicaciones a una cuenta de usuario

Si necesita controlar las aplicaciones en el nivel de usuario, puede asignar aplicaciones o grupos de aplicaciones a cuentas de usuario. Cuando se asigna una aplicación a un usuario, la aplicación está disponible para cualquier dispositivo que el usuario haya activado para ese tipo de dispositivo y la aplicación aparece en el catálogo de aplicaciones de trabajo en el dispositivo.

También puede asignar aplicaciones a los usuarios para tipos de dispositivo que el usuario no haya activado todavía. Si el usuario activa un tipo de dispositivo diferente en el futuro, las aplicaciones adecuadas estarán disponibles para el dispositivo nuevo del usuario.

La misma aplicación puede asignarse directamente a la cuenta de usuario o puede heredarse de grupos de usuarios o de dispositivos. La configuración de la aplicación (por ejemplo, si la aplicación es obligatoria) se asigna en función de la prioridad: los grupos de dispositivos tienen la prioridad más alta, a continuación, las cuentas de usuario y, por último, los grupos de usuarios.

Antes de empezar: Adición de las aplicaciones a un grupo de aplicaciones.

1. En la barra de menú, haga clic en **Usuarios > Dispositivos gestionados**.
2. Busque una cuenta de usuario.
3. En los resultados de la búsqueda, haga clic en el nombre de una cuenta de usuario.
4. En la sección **Aplicaciones**, haga clic en +.
5. Seleccione la casilla de verificación junto a las aplicaciones o el grupo de aplicaciones que desea asignar a la cuenta del usuario.
6. Haga clic en **Siguiente**.
7. En la lista desplegable **Disposición** de la aplicación, realice una de las acciones siguientes:
   - Para obligar a los usuarios a instalar la aplicación, seleccione **Obligatorio**.
   - Para permitir a los usuarios instalar y eliminar la aplicación, seleccione **Opcional**.

     Nota: Si la misma aplicación se asigna a una cuenta de usuario, un grupo de usuarios al que pertenece el usuario y el grupo de dispositivos al que pertenece el dispositivo, tiene prioridad la disposición de la aplicación asignada al grupo de dispositivos.
8. En los dispositivos iOS, para asignar los ajustes de VPN por aplicación a una aplicación o grupo de aplicaciones, en la lista desplegable **VPN por aplicación** para la aplicación o grupo de aplicaciones, seleccione los ajustes que desea asociar a la aplicación o grupo de aplicaciones.
9. Si agrega una aplicación iOS, realice una de las tareas siguientes:

Tarea	Pasos
Si no ha agregado una cuenta de VPP o no va a agregar una aplicación iOS	**a.** Haga clic en **Asignar**.

Tarea	Pasos
Si va a agregar una aplicación iOS y ha agregado al menos una cuenta de VPP	**a.** Haga clic en **Siguiente**. **b.** Seleccione **Sí** si desea asignar una licencia a la aplicación iOS. Seleccione **No** si no desea asignar una licencia o no tiene una licencia que asignar a la aplicación. **c.** Si ha asignado una licencia a la aplicación, en la lista desplegable **Licencia de la aplicación**, seleccione la cuenta de VPP para asociarla a la aplicación. **d.** En la lista desplegable **Asignar licencia a**, asigne la licencia al **Usuario** o al **Dispositivo**. Si no se especifica el valor en la lista desplegable **Licencia de la aplicación**, la lista desplegable **Asignar licencia a** no está disponible. **e.** Haga clic en **Asignar**. Los usuarios deben seguir las instrucciones para inscribirse en el programa de compras por volumen (VPP) en los dispositivos de la empresa antes de poder instalar aplicaciones de prepago. Los usuarios deben completar esta tarea una vez **Nota:** Si concede acceso a un número de licencias superior al número de licencias disponibles, los primeros usuarios que accedan a las licencias disponibles podrán instalar la aplicación. Si la aplicación es una aplicación obligatoria que no tiene una licencia disponible, debe obtener la licencia antes de que el usuario pueda instalar la aplicación o estará sujeto a las reglas de cumplimiento que se hayan asignado al usuario.

Referencia relacionada

Comportamiento de la aplicación en los dispositivos Android
Comportamiento de la aplicación en los dispositivos iOS
Comportamiento de la aplicación en los dispositivos BlackBerry

Asignación de una política de TI de BlackBerry OS, un perfil o una configuración de software a una cuenta de usuario

Antes de empezar:

- Compruebe haber activado la activación del dispositivo con BlackBerry OS para la cuenta de usuario. Para obtener más información, descargue la Guía de administración en help.blackberry.com/detectLang/bes5-for-exchange/.
- Cree una política de TI de BlackBerry OS.
- Cree una configuración de software.
- Cree un perfil de Wi-Fi o de VPN para los dispositivos con BlackBerry OS. Para obtener más información, descargue la Guía de administración en help.blackberry.com/detectLang/bes5-for-exchange/.
- Cree una regla de control de acceso de inserción o de extracción para los dispositivos con BlackBerry OS. Para obtener más información, descargue la Guía de administración en help.blackberry.com/detectLang/bes5-for-exchange/.

1. En la barra de menú, haga clic en **Usuarios**.
2. Busque una cuenta de usuario.
3. En los resultados de la búsqueda, haga clic en el nombre de la cuenta de usuario.
4. En la sección **Política de TI, perfiles y configuraciones de software**, haga clic en +.

5. Haga clic en **Política de TI**, **Wi-Fi**, **VPN**, **Regla de control de acceso de inserción**, **Regla de control de acceso de extracción** o **Configuración de software**.
6. En la lista desplegable, haga clic en el nombre de la política de TI, el perfil, la regla de control de acceso o la configuración de software que desea asignar al usuario.
7. Haga clic en **Asignar**.

Conceptos relacionados

Control de las capacidades del dispositivo con BlackBerry OS mediante políticas de TI

Tareas relacionadas

Asignación de una política de TI de BlackBerry OS, un perfil o una configuración de software a un grupo de usuarios

Presentación de las reglas de políticas de TI de BlackBerry OS resueltas que se asignan a una cuenta de usuario

Si un usuario es miembro de varios grupos de usuarios que tienen diferentes políticas de TI de BlackBerry OS, BlackBerry UEM resuelve los conflictos de las políticas de TI o la configuración de la regla de política de TI mediante el método de reconciliación que se ha especificado en la configuración de BlackBerry OS. Puede ver los resultados de la reconciliación de la política de TI de BlackBerry OS y los ajustes resueltos para cada regla en Configuración avanzada de la pestaña Resumen. Si una regla de política de TI es la misma en las distintas políticas de TI de BlackBerry OS que se aplican a la cuenta de usuario, los resultados no muestran la regla de política de TI.

1. En la barra de menú, haga clic en **Usuarios**.
2. Busque una cuenta de usuario.
3. En los resultados de la búsqueda, haga clic en el nombre de la cuenta de usuario.
4. En la sección **Política de TI, perfiles y configuraciones de software**, haga clic en **Configuración avanzada**.
5. Haga clic en la pestaña **Políticas**.
6. En la sección **Nombre de la política de TI resuelto**, haga clic en el nombre de la política de TI de BlackBerry OS.

Creación y administración de grupos de usuarios

Un grupo de usuarios es un conjunto de usuarios relacionados que comparten propiedades comunes. La administración de usuarios como un grupo es más eficaz que la administración individual, ya que las propiedades de los usuarios se pueden agregar, modificar o eliminar para todos los miembros del grupo al mismo tiempo.

Los usuarios pueden pertenecer a más de un grupo a la vez. Puede asignar una política de TI, perfiles y aplicaciones en la consola de gestión al crear o actualizar los ajustes para un grupo de usuarios. Si el dominio BlackBerry UEM es compatible con los dispositivos con BlackBerry OS (de la versión 5.0 a la 7.1), puede asignar una política de TI, perfiles y configuraciones de software de BlackBerry OS.

Puede crear dos tipos de grupos de usuarios:

- Los grupos vinculados a directorios se vinculan a grupos del directorio de la empresa. Solo las cuentas de usuario del directorio pueden ser miembros de un grupo vinculado al directorio.
- Los grupos locales se crean y se mantienen en BlackBerry UEM y pueden tener cuentas de usuario locales y cuentas de usuario del directorio asignadas.

Después de crear grupos de usuarios, puede definir un grupo como un miembro de otro grupo. Cuando anida un grupo dentro de un grupo de usuarios, los miembros del grupo anidado heredarán las propiedades del grupo de usuarios. Cree y mantenga la estructura de anidamiento en BlackBerry UEM y podrá anidar tanto en grupos vinculados a directorios como en grupos locales dentro de cada tipo de grupo de usuarios.

Creación de grupos vinculados a directorios

Puede crear grupos en BlackBerry UEM que estén vinculados a uno o más grupos en el directorio de la empresa. Estos grupos de BlackBerry UEM se denominan "grupos vinculados a directorios". Solo las cuentas de usuario de directorio pueden ser miembros de un grupo vinculados a directorios.

En un intervalo programado, BlackBerry UEM sincroniza automáticamente la pertenencia de un grupo vinculado a directorios con el grupo de directorios de la empresa asociado (o grupos). Los usuarios que se han agregado o eliminado del grupo de directorios de la empresa se agregan o se eliminan del grupo vinculado a directorios.

Nota: Cuando los usuarios se mueven a un grupo de directorios de la empresa que está vinculado a un grupo vinculado a directorios, se les asignan las políticas, los perfiles y las aplicaciones que están asignados al grupo. Cuando se eliminan usuarios de un grupo de directorios de la empresa que está vinculado a un grupo vinculado a directorios, las políticas, los perfiles y las aplicaciones se eliminan del usuario.

Cada grupo vinculado a directorios puede vincularse a un único directorio de la empresa. Por ejemplo, si BlackBerry UEM tiene dos conexiones de Microsoft Active Directory, (A y B), y crea un grupo vinculado a directorios que está vinculado a una conexión A, solo podrá vincularlo a grupos de directorios de la conexión A. Debe crear nuevos grupos vinculados a directorios para cualquier conexión de directorio.

Para activar esta función, consulte "Permitir los grupos vinculados a directorios" en el contenido de Configuración.

Sincronizar grupos vinculados a directorios no agregan ni eliminan usuarios en BlackBerry UEM. Para permitir que BlackBerry UEM cree cuentas de usuario cuando se creen nuevos usuarios de directorios de la empresa, debe activar y configurar la integración. Para obtener más información, consulte "Permitir integración" en el contenido de Configuración.

Creación de un grupo vinculado a directorios

Antes de empezar: Permitir los grupos vinculados al directorio. Para obtener más instrucciones, consulte el contenido de Configuración.

1. En la barra de menús, haga clic en **Grupos**.

2. Haga clic en .
3. Escriba el nombre del grupo.
4. En la sección **Grupos vinculados al directorio**, realice las acciones siguientes:
   a) Haga clic en +.
   b) Escriba el nombre o parte del nombre del grupo de directorio de la empresa al que quiera vincularse.
   c) Si tiene más de una conexión de directorio de la empresa, seleccione la conexión que desea buscar. Tras haber realizado esta selección, el grupo vinculado a directorios se asociará permanentemente a la conexión seleccionada.
   d) Haga clic en .
   e) Seleccione el grupo de directorios de la empresa en la lista de resultados de la búsqueda.
   f) Haga clic en **Agregar**. El grupo de directorio de la empresa se muestra en la lista y la conexión de directorio de la empresa a la que está vinculada el grupo se muestra al lado del título de la sección.
   g) Si fuera necesario, seleccione la casilla de verificación **Vincular grupos anidados**. Puede dejar sin seleccionar la casilla de verificación para vincular a todos los grupos anidados o puede seleccionarla para permitir que la configuración del directorio controle el número de grupos anidados.
   h) Repita estos pasos para vincular grupos adicionales.
5. Para asignar una función de usuario al grupo vinculado a directorios, realice las siguientes acciones:
   a) En la sección **Función de usuario**, haga clic en +
   b) En la lista desplegable, haga clic en el nombre de la función de usuario que desea asignar al grupo.
   c) Haga clic en **Agregar**.
6. Para asignar una política de TI o un perfil al grupo vinculado a directorios, realice las acciones siguientes:
   a) En la sección **Política de TI y perfiles**, haga clic en +.
   b) Haga clic en **Política de TI** o en un tipo de perfil.
   c) En la lista desplegable, haga clic en el nombre de la política de TI o del perfil que desea asignar al grupo.
   d) Haga clic en **Asignar**.
7. Para asignar una aplicación al grupo vinculado a directorios, en la sección **Aplicaciones asignadas**, haga clic en +.
8. Busque la aplicación.
9. En los resultados de la búsqueda, seleccione la aplicación.
10. Haga clic en **Siguiente**.
11. En la lista desplegable **Disposición** de la aplicación, realice una de las acciones siguientes:
    - Para instalar la aplicación automáticamente en los dispositivos e impedir que los usuarios la eliminen, seleccione **Obligatorio**. Esta opción no está disponible para las aplicaciones de BlackBerry.
    - Para permitir que los usuarios instalen y eliminen la aplicación, seleccione **Opcional**.
12. En los dispositivos iOS, para asignar los ajustes de VPN por aplicación a una aplicación o grupo de aplicaciones, en la lista desplegable **VPN por aplicación** para la aplicación o grupo de aplicaciones, seleccione los ajustes que desea asociar a la aplicación o grupo de aplicaciones.
13. Haga clic en **Asignar**.
14. Haga clic en **Agregar**.

Tareas relacionadas

Creación de un grupo local

Adición de un grupo de directorios de la empresa a un grupo vinculado a directorios

1. En la barra de menús, haga clic en **Grupos**.
2. Haga clic en el grupo vinculado a directorios.
3. Haga clic en la pestaña **Configuración**.
4. Haga clic en .
5. En la sección **Grupos vinculados al directorio**, haga clic en .
6. Escriba el nombre del grupo de directorios de la empresa.
7. Haga clic en **Buscar**.
8. Seleccione el grupo de directorios de la empresa en la lista de resultados de la búsqueda.
9. Haga clic en **Agregar**.
10. Si fuera necesario, seleccione **Vincular grupos anidados**.

Creación de un grupo local

1. En la barra de menús, haga clic en **Grupos**.
2. Haga clic en .
3. Escriba un nombre para el grupo de usuarios.
4. De manera opcional, puede escribir una descripción para el grupo de usuarios.
5. Para asignar una función de usuario al grupo local, realice las siguientes acciones:
   a) En la sección **Función de usuario**, haga clic en .
   b) En la lista desplegable, haga clic en el nombre de la función de usuario que desea asignar al grupo.
   c) Haga clic en **Agregar**.
6. Para asignar una política de TI o el perfil al grupo local, realice las siguientes acciones:
   a) En la sección **Política de TI y perfiles**, haga clic en .
   b) Haga clic en **Política de TI** o en un tipo de perfil.
   c) En la lista desplegable, haga clic en el nombre de la política de TI o del perfil que desea asignar al grupo.
   d) Haga clic en **Asignar**.
7. Para asignar una aplicación al grupo de usuarios, en la sección **Aplicaciones asignadas**, haga clic en .
8. Busque la aplicación.
9. En los resultados de la búsqueda, seleccione la aplicación.
10. Haga clic en **Siguiente**.
11. En la lista desplegable **Disposición** de la aplicación, realice una de las acciones siguientes:
    - Para instalar la aplicación automáticamente en los dispositivos e impedir que los usuarios la eliminen, seleccione **Obligatorio**. Esta opción no está disponible para las aplicaciones de BlackBerry.
    - Para permitir a los usuarios instalar y eliminar la aplicación, seleccione **Opcional**.

      Nota: Si la misma aplicación se asigna a una cuenta de usuario y al grupo de usuarios al que pertenece el usuario, tiene prioridad la disposición de la aplicación asignada a la cuenta de usuario.
12. En los dispositivos iOS, para asignar los ajustes de VPN por aplicación a una aplicación o grupo de aplicaciones, en la lista desplegable **VPN por aplicación** para la aplicación o grupo de aplicaciones, seleccione los ajustes que desea asociar a la aplicación o grupo de aplicaciones.
13. Haga clic en **Asignar**.
14. Cuando termine de especificar las propiedades del grupo de usuarios, haga clic en **Agregar**.

Tareas relacionadas

Creación de un grupo vinculado a directorios
Agregar usuarios a los grupos de usuarios

Consulta de un grupo de usuarios

1. En la barra de menús, haga clic en **Grupos**.
2. Busque un grupo de usuarios.
3. En los resultados de la búsqueda, haga clic en el nombre del grupo de usuarios.
4. Para ver los miembros de un grupo de usuarios, realice las acciones siguientes:
   a) Haga clic en **Usuarios** para ver las cuentas de usuario asignadas.
   b) Haga clic en **Grupos anidados** para ver los grupos anidados asignados.
5. Haga clic en **Configuración** para ver la información siguiente sobre un grupo de usuarios:
   - Grupos vinculados al directorio (disponible para un grupo vinculado a directorios)
   - Asignación de la política de TI, los perfiles y las configuraciones de software de BlackBerry OS (disponibles si el dominio de BlackBerry UEM es compatible con los dispositivos con BlackBerry OS)
   - Asignación de la política de TI, de perfiles y de aplicaciones

Cambio del nombre de un grupo de usuarios

1. En la barra de menús, haga clic en **Grupos**.
2. Busque el grupo de usuarios que desea ver.
3. Haga clic en el grupo de usuarios.
4. Haga clic en .
5. Cambie el nombre del grupo de usuarios.
6. De forma opcional, cambie la descripción del grupo de usuarios.
7. Haga clic en **Guardar**.

Eliminar un grupo de usuarios

Al eliminar un grupo de usuarios, los usuarios del grupo no se eliminan. Las propiedades del grupo que se asignan al usuario se han eliminado o modificado.

1. En la barra de menús, haga clic en **Grupos**.
2. Busque el grupo de usuarios que desea eliminar.
3. Haga clic en el grupo de usuarios.
4. Haga clic en .
5. Haga clic en **Eliminar**.

Adición de grupos anidados a un grupo de usuarios

Al agregar un grupo anidado a un grupo de usuarios, cualquiera de los grupos a los que pertenece el grupo anidado se agregarán también.

Antes de empezar: Cree grupos de usuarios. Puede crear grupos vinculados a directorios o grupos locales.

1. En la barra de menús, haga clic en **Grupos**.
2. Busque un grupo de usuarios.
3. En los resultados de la búsqueda, haga clic en el nombre del grupo de usuarios.

4. Haga clic en la pestaña **Grupos anidados**.
5. Haga clic en +.
6. Seleccione uno o más grupos disponibles.
7. Haga clic en **Agregar**.

Eliminación de grupos anidados de un grupo de usuarios

Puede eliminar grupos anidados que se asignan directamente a un grupo de usuarios.

1. En la barra de menús, haga clic en **Grupos**.
2. Busque un grupo de usuarios.
3. En los resultados de la búsqueda, haga clic en el nombre del grupo de usuarios.
4. Haga clic en la pestaña **Grupos anidados**.
5. Haga clic en ✕ junto a cada grupo anidado que desea eliminar.

Asignación de un perfil o una política de TI a un grupo de usuarios

1. En la barra de menú, haga clic en **Grupos > Usuario**.
2. En la lista de grupos, haga clic en el nombre del grupo de usuarios.
3. En la sección **Perfil asignado**, haga clic en +.
4. Haga clic en **Política de TI** o en un tipo de perfil.
5. En la lista desplegable, haga clic en el nombre del perfil o la política de TI que desea asignar al grupo.
6. Para las políticas de TI y la clasificación de los tipos de perfil, si el tipo de perfil que ha seleccionado en el paso 6 ya está asignado directamente al grupo, haga clic en **Sustituir**. De lo contrario, haga clic en **Asignar**.

Conceptos relacionados

¿Cómo elige BlackBerry UEM qué política de TI asignar?
Asignación de perfiles
¿Cómo elige BlackBerry UEM qué perfiles asignar?

Tareas relacionadas

Creación de una política de TI
Crear un perfil de requisitos de solicitud de servicio del dispositivo para dispositivos con BlackBerry 10
Asignar un perfil o una política de TI a una cuenta de usuario

Asignación de una aplicación a un grupo de usuarios

Al asignar aplicaciones a un grupo de usuarios, las aplicaciones están disponibles para cualquiera de los dispositivos aplicables que los miembros del grupo de usuarios hayan activado. También puede asignar aplicaciones a los grupos de usuarios para tipos de dispositivo que los miembros del grupo de usuarios no hayan activado todavía. Esto asegura que si cualquier miembro del grupo activa un tipo de dispositivo diferente en el futuro, las aplicaciones adecuadas estarán disponibles para nuevos dispositivos.

Si una cuenta de usuario es miembro de varios grupos de usuarios que tienen las mismas aplicaciones o grupos de aplicaciones asignados a ellos, solo una instancia de la aplicación o el grupo de aplicaciones aparece en la lista de las aplicaciones asignadas para dicha cuenta de usuario. La misma aplicación puede asignarse directamente a la cuenta de usuario o puede heredarse de grupos de usuarios o de dispositivos. La configuración de la aplicación (por ejemplo, si la aplicación es necesaria) se asigna en función de la prioridad. Los grupos

de dispositivos tienen la prioridad más alta, a continuación, las cuentas de usuario y, después, los grupos de usuarios.

Antes de empezar:

- Adición de la aplicación a la lista de aplicaciones disponibles.
- Opcionalmente, adición de las aplicaciones a un grupo de aplicaciones.

1. En la barra de menú, haga clic en **Grupos > Usuario**.
2. En la lista de grupos, haga clic en el nombre del grupo de usuarios.
3. En la sección **Aplicaciones asignadas**, haga clic en +.
4. En el campo Buscar, escriba el nombre de la aplicación, el proveedor o la URL de la aplicación que desea agregar.
5. Seleccione la casilla de verificación junto a las aplicaciones o el grupo de aplicaciones que desea asignar al grupo de usuarios.
6. Haga clic en **Siguiente**.
7. En la lista desplegable **Disposición** de la aplicación, realice una de las acciones siguientes:
   - Para obligar a los usuarios a instalar la aplicación, seleccione **Obligatorio**.
   - Para permitir a los usuarios instalar y eliminar la aplicación, seleccione **Opcional**.

   Nota: Si la misma aplicación se asigna a una cuenta de usuario, un grupo de usuarios al que pertenece el usuario y el grupo de dispositivos al que pertenece el dispositivo, tiene prioridad la disposición de la aplicación asignada al grupo de dispositivos.
8. En los dispositivos iOS, para asignar los ajustes de VPN por aplicación a una aplicación o grupo de aplicaciones, en la lista desplegable **VPN por aplicación** para la aplicación o grupo de aplicaciones, seleccione los ajustes que desea asociar a la aplicación o grupo de aplicaciones.
9. Para dispositivos iOS y Android, si hay disponible una configuración de aplicaciones, seleccione la configuración de aplicaciones que desee asignar a la aplicación.
10. Lleve a cabo una de las tareas siguientes:

Tarea	Pasos
Si no ha agregado una cuenta de VPP o no va a agregar una aplicación iOS	**a.** Haga clic en **Asignar**.

Tarea	Pasos
Si va a agregar una aplicación iOS y ha agregado al menos una cuenta de VPP	**a.** Haga clic en **Next (Siguiente)**. **b.** Seleccione **Sí** si desea asignar una licencia a la aplicación iOS. Seleccione **No** si no desea asignar una licencia o no tiene una licencia que asignar a la aplicación. **c.** Si ha asignado una licencia a la aplicación, en la lista desplegable **Licencia de la aplicación**, seleccione la cuenta de VPP para asociarla a la aplicación. **d.** En la lista desplegable **Asignar licencia a**, asigne la licencia al **Usuario** o al **Dispositivo**. Si no se especifica el valor en la lista desplegable **Licencia de la aplicación**, la lista desplegable **Asignar licencia a** no está disponible. **e.** Haga clic en **Asignar**. Los usuarios deben seguir las instrucciones para inscribirse en el programa de compras por volumen (VPP) en los dispositivos de la empresa antes de poder instalar aplicaciones de prepago. Los usuarios deben completar esta tarea una vez. **Nota:** Si concede acceso a un número de licencias superior al número de licencias disponibles, los primeros usuarios que accedan a las licencias disponibles podrán instalar la aplicación. Si la aplicación es una aplicación obligatoria que no tiene una licencia disponible, debe obtener la licencia antes de que el usuario pueda instalar la aplicación o dicho usuario estará sujeto a las reglas de cumplimiento que se hayan asignado al usuario.

Referencia relacionada

Comportamiento de la aplicación en los dispositivos Android
Comportamiento de la aplicación en los dispositivos iOS
Comportamiento de la aplicación en los dispositivos BlackBerry

Asignación de un grupo de aplicaciones a un grupo de usuarios

Al asignar un grupo de aplicaciones a un grupo de usuarios, las aplicaciones están disponibles para cualquiera de los dispositivos aplicables que los miembros del grupo de usuarios hayan activado. También puede asignar aplicaciones a los grupos de usuarios para tipos de dispositivo que los miembros del grupo de usuarios no hayan activado todavía. Esto asegura que si cualquier miembro del grupo activa un tipo de dispositivo diferente en el futuro, las aplicaciones adecuadas estarán disponibles para nuevos dispositivos.

Si una cuenta de usuario es miembro de varios grupos de usuarios que tienen las mismas aplicaciones o grupos de aplicaciones asignadas a ellos, solo una instancia del grupo de aplicaciones aparece en la lista de las aplicaciones asignadas para dicha cuenta de usuario. La misma aplicación puede asignarse directamente a la cuenta de usuario o puede heredarse de grupos de usuarios o de dispositivos. La configuración de la aplicación (por ejemplo, si la aplicación es obligatoria) se asigna en función de la prioridad: los grupos de dispositivos tienen la prioridad más alta, a continuación, las cuentas de usuario y, por último, los grupos de usuarios.

Antes de empezar:

- Adición de las aplicaciones a un grupo de aplicaciones.

1. En la barra de menús, haga clic en **Grupos**.
2. En la pestaña **Grupos de usuario**, haga clic en el nombre de un grupo.
3. En la sección **Aplicaciones asignadas**, haga clic en +.

4. En el campo de búsqueda, escriba el nombre del grupo de aplicaciones que desea agregar.
5. Seleccione la casilla de verificación junto a las aplicaciones o el grupo de aplicaciones que desea asignar al grupo de usuarios.
6. Haga clic en **Siguiente**.
7. En la lista desplegable **Disposición** de la aplicación, realice una de las acciones siguientes:
   - Para obligar a los usuarios a instalar la aplicación, seleccione **Obligatorio**.
   - Para permitir a los usuarios instalar y eliminar la aplicación, seleccione **Opcional**.

   Nota: Si la misma aplicación se asigna a una cuenta de usuario, un grupo de usuarios al que pertenece el usuario y el grupo de dispositivos al que pertenece el dispositivo, tiene prioridad la disposición de la aplicación asignada al grupo de dispositivos.
8. En los dispositivos iOS, para asignar los ajustes de VPN por aplicación a una aplicación o grupo de aplicaciones, en la lista desplegable **VPN por aplicación** para la aplicación o grupo de aplicaciones, seleccione los ajustes que desea asociar a la aplicación o grupo de aplicaciones.
9. Lleve a cabo una de las tareas siguientes:

Tarea	Pasos
Si no ha agregado una cuenta de VPP o no va a agregar una aplicación iOS	**a.** Haga clic en **Asignar**.
Si va a agregar una aplicación iOS y ha agregado al menos una cuenta de VPP	**a.** Haga clic en **Siguiente**. **b.** Seleccione **Sí** si desea asignar una licencia a la aplicación iOS. Seleccione **No** si no desea asignar una licencia o no tiene una licencia que asignar a la aplicación. **c.** Si ha asignado una licencia a la aplicación, en la lista desplegable **Licencia de la aplicación**, seleccione la cuenta de VPP para asociarla a la aplicación. **d.** En la lista desplegable **Asignar licencia a**, asigne la licencia al **Usuario** o al **Dispositivo**. Si no se especifica el valor en la lista desplegable **Licencia de la aplicación**, la lista desplegable **Asignar licencia a** no está disponible. **e.** Haga clic en **Asignar**. Los usuarios deben seguir las instrucciones para inscribirse en el programa de compras por volumen (VPP) en los dispositivos de la empresa antes de poder instalar aplicaciones de prepago. Los usuarios deben completar esta tarea una vez. **Nota:** Si concede acceso a un número de licencias superior al número de licencias disponibles, los primeros usuarios que accedan a las licencias disponibles podrán instalar la aplicación. Si la aplicación es una aplicación obligatoria que no tiene una licencia disponible, debe obtener la licencia antes de que el usuario pueda instalar la aplicación o dicho usuario estará sujeto a las reglas de cumplimiento que se hayan asignado al usuario.

Referencia relacionada

Comportamiento de la aplicación en los dispositivos Android
Comportamiento de la aplicación en los dispositivos iOS
Comportamiento de la aplicación en los dispositivos BlackBerry

Asignación de una política de TI de BlackBerry OS, un perfil o una configuración de software a un grupo de usuarios

Antes de empezar:

- Cree una política de TI de BlackBerry OS. Para obtener más información, descargue la Guía de administración en help.blackberry.com/detectLang/bes5-for-exchange/.
- Cree una configuración de software.
- Cree un perfil de Wi-Fi o de VPN para los dispositivos con BlackBerry OS. Para obtener más información, descargue la Guía de administración en help.blackberry.com/detectLang/bes5-for-exchange/.
- Cree una regla de control de acceso de inserción o de extracción para los dispositivos con BlackBerry OS. Para obtener más información, descargue la Guía de administración en help.blackberry.com/detectLang/bes5-for-exchange/.

1. En la barra de menús, haga clic en **Grupos**.
2. Busque un grupo de usuarios.
3. En los resultados de la búsqueda, haga clic en el nombre del grupo de usuarios.
4. Haga clic en la pestaña **Dispositivos gestionados**.
5. En la sección **Política de TI, perfiles y configuraciones de software**, haga clic en +.
6. Haga clic en **Política de TI**, **Wi-Fi**, **VPN**, **Regla de control de acceso de inserción**, **Regla de control de acceso de extracción** o **Configuración de software**.
7. En la lista desplegable, haga clic en el nombre de la política de TI, el perfil, la regla de control de acceso o la configuración de software que desea asignar al grupo.
8. Haga clic en **Asignar**.

Conceptos relacionados

Control de las capacidades del dispositivo con BlackBerry OS mediante políticas de TI

Tareas relacionadas

Asignación de una política de TI de BlackBerry OS, un perfil o una configuración de software a una cuenta de usuario

Creación y gestión de grupos de dispositivos compartidos

Puede permitir que varios usuarios compartan un dispositivo iOS y configurar los ajustes específicos de cada usuario o los mismos para todos los usuarios. Puede personalizar los términos de uso que los usuarios deben aceptar para desinscribir dispositivos compartidos. Un usuario puede desinscribir un dispositivo utilizando la autenticación local o de Microsoft Active Directory. Cuando termine de utilizarlo, puede inscribirlo y el dispositivo estará disponible para el siguiente usuario. Los dispositivos gestionados siguen siendo gestionados por BlackBerry UEM durante el proceso de desinscripción e inscripción.

Esta función se ha diseñado para dispositivos supervisados con la configuración siguiente:

- Modo de bloqueo de la aplicación activado
- Aplicaciones de VPP asignadas

Nota: Esta función no es compatible con aplicaciones de BlackBerry Dynamics. Se debe asignar el mismo perfil de BlackBerry Dynamics a la cuenta de usuario propietaria del grupo de dispositivos compartidos y también al grupo de dispositivos compartidos. Debe comprobar que la opción "Activar UEM Client para que pueda inscribirse en BlackBerry Dynamics" no esté seleccionada en el perfil.

Conceptos relacionados

Limitación de los dispositivos a una única aplicación
Gestión de las cuentas de VPP de Apple

Crear un grupo de dispositivos compartidos

Al crear un grupo de dispositivos compartidos, se crea una cuenta de usuario local. Esta cuenta de usuario local es la propietaria del grupo de dispositivos compartidos.

1. En la barra de menú, haga clic en **Usuarios > Grupos de dispositivos compartidos**.
2. Haga clic en + junto al a barra de búsqueda.
3. Escriba un nombre para el grupo de dispositivos compartidos.
4. De manera opcional, puede escribir una descripción para el grupo de dispositivos compartidos.
5. Escriba el nombre de usuario para la activación de los dispositivos.
6. Para solicitar a los usuarios que acepten los términos de servicio cuando desinscriban un dispositivo compartido, debe realizar las acciones siguientes:
   a) Seleccione **Activar términos del servicio**.
   b) Escriba el texto de los términos de servicio.
7. En la sección **Usuarios concedidos**, busque un usuario y haga clic en su nombre en la lista de resultados de la búsqueda.
8. Repita el paso 7 para cada usuario que desee agregar.
9. Haga clic en **Guardar**.

Después de terminar: Para activar el bloqueo de la aplicación UEM Client, edite la información del grupo de dispositivos compartidos.

Activar un dispositivo compartido

Para que los usuarios puedan desinscribir dispositivos compartidos, debe activarlos.

Antes de empezar: Compruebe que el perfil de BlackBerry Dynamics asignado al grupo de dispositivos compartidos no tiene seleccionada la opción **Activar UEM Client para que pueda inscribirse en BlackBerry**

Dynamics. Compruebe que el mismo perfil también se ha asignado a la cuenta de usuario propietaria del grupo de dispositivos compartidos.

1. En la barra de menú, haga clic en **Usuarios > Dispositivos compartidos**.
2. Busque un grupo de dispositivos compartidos.
3. En los resultados de la búsqueda, haga clic en el nombre del grupo de dispositivos compartidos.
4. Haga clic en **Activación del dispositivo** para ver la dirección del servidor y el nombre de usuario y la contraseña de activación.
5. Utilice la información de autenticación del dispositivo para activar el dispositivo. Para obtener ayuda con la activación, consulte Activar un dispositivo iOS .

Después de terminar: Compruebe que el dispositivo activado se muestra en la sección **Dispositivos compartidos**. BlackBerry UEM utiliza el nombre del grupo para generar el nombre de dispositivo y agrega un número. Por ejemplo, si el nombre del grupo es Ejemplo, el primer dispositivo que active se denomina Ejemplo 01.

Ver el historial de desinscripciones de un usuario

Puede ver la lista de dispositivos compartidos que ha utilizado un usuario. Cada registro indica las veces que se ha desinscrito e inscrito un dispositivo y la lista muestra los últimos 50 registros de un usuario. El historial de desinscripciones de un usuario se actualiza cuando este inscribe un dispositivo.

1. En la barra de menú, haga clic en **Usuarios > Dispositivos compartidos**.
2. Busque un grupo de dispositivos compartidos.
3. En los resultados de la búsqueda, haga clic en el nombre del grupo de dispositivos compartidos.
4. En la sección **Usuarios concedidos**, haga clic en **Ver** en la columna **Historial de anulaciones** del usuario.

Editar la suscripción de usuarios para un grupo de dispositivos compartidos

La suscripción de usuarios para un grupo de dispositivos compartidos especifica la lista de usuarios con acceso a los dispositivos compartidos activados para el grupo. Los usuarios pueden pertenecer a uno o más grupos de dispositivos compartidos.

1. En la barra de menú, haga clic en **Usuarios > Dispositivos compartidos**.
2. Busque un grupo de dispositivos compartidos.
3. En los resultados de la búsqueda, haga clic en el nombre del grupo de dispositivos compartidos.
4. En la sección **Usuarios concedidos**, realice una de las siguientes acciones:
   - Para agregar un usuario al grupo, busque al usuario y haga clic en su nombre en la lista de resultados de la búsqueda.
   - Para eliminar un usuario del grupo, haga clic en ✕ en la columna **Acción** del usuario y haga clic en **Enviar**.
5. Repita el paso 4 para cada usuario que desee agregar o eliminar.

Eliminar un dispositivo del grupo de dispositivos compartidos

Al eliminar un dispositivo de un grupo de dispositivos compartidos, BlackBerry UEM envía el comando Eliminar solo los datos de trabajo al dispositivo.

1. En la barra de menú, haga clic en **Usuarios > Dispositivos compartidos**.
2. Busque un grupo de dispositivos compartidos.
3. En los resultados de la búsqueda, haga clic en el nombre del grupo de dispositivos compartidos.
4. En la sección **Dispositivos compartidos**, lleve a cabo las siguientes acciones:
   a) Haga clic en ✕ en la columna **Acción** del dispositivo.
   b) Haga clic en **Eliminar solo los datos de trabajo**.

5. Repita el paso 4 para cada dispositivo que desee eliminar.

Eliminar un grupo de dispositivos compartidos

Antes de empezar: Elimine todos los dispositivos del grupo de dispositivos compartidos.

1. En la barra de menú, haga clic en **Usuarios > Dispositivos compartidos**.
2. Busque un grupo de dispositivos compartidos.
3. En los resultados de la búsqueda, haga clic en el nombre del grupo de dispositivos compartidos.
4. Haga clic en 🗑.
5. Haga clic en **Eliminar**.

Asignar una aplicación a un grupo de dispositivos compartidos

Al asignar aplicaciones o grupos de aplicaciones a un grupo de dispositivos compartidos, las aplicaciones están disponibles cuando un usuario desinscribe un dispositivo que está activado para el grupo y se eliminan cuando el usuario inscribe el dispositivo. Si desea que algunas aplicaciones permanezcan en los dispositivos cuando se inscriben, también debe asignar las aplicaciones a la cuenta de usuario propietaria del grupo de dispositivos compartidos.

Antes de empezar:

- Adición de la aplicación a la lista de aplicaciones disponibles.
- Opcionalmente, adición de las aplicaciones a un grupo de aplicaciones.

1. En la barra de menú, haga clic en **Usuarios > Dispositivos compartidos**.
2. Busque un grupo de dispositivos compartidos.
3. En los resultados de la búsqueda, haga clic en el nombre del grupo de dispositivos compartidos.
4. En la sección **Aplicaciones asignadas**, haga clic en +.
5. En el campo Buscar, escriba el nombre de la aplicación, el proveedor o la URL de la aplicación que desea agregar.
6. Seleccione la casilla de verificación junto a las aplicaciones o el grupo de aplicaciones que desea asignar al grupo de usuarios.
7. Haga clic en **Siguiente**.
8. En la lista desplegable **Disposición** de la aplicación, realice una de las acciones siguientes:
   - Para obligar a los usuarios a instalar la aplicación, seleccione **Obligatorio**.
   - Para permitir que los usuarios instalen y eliminen la aplicación, seleccione **Opcional**.
9. Para asignar los ajustes de VPN por aplicación a una aplicación o grupo de aplicaciones, en la lista desplegable **VPN por aplicación** para la aplicación o grupo de aplicaciones, seleccione los ajustes que desea asociar a la aplicación o grupo de aplicaciones.
10. Si hay disponible una configuración de aplicaciones, seleccione la configuración de aplicaciones que desee asignar a la aplicación.
11. Haga clic en **Siguiente**.
12. Seleccione **Sí** si desea asignar una licencia a la aplicación. Seleccione **No** si no desea asignar una licencia o no tiene una licencia que asignar a la aplicación.
13. Si ha asignado una licencia a la aplicación, en la lista desplegable **Licencia de la aplicación**, seleccione la cuenta de VPP para asociarla a la aplicación.
14. En la lista desplegable **Asignar licencia a**, asigne la licencia al **Usuario** o al **Dispositivo**. Si no se especifica el valor en la lista desplegable **Licencia de la aplicación**, la lista desplegable **Asignar licencia a** no está disponible.

15. Haga clic en **Asignar**.

    Los usuarios deben seguir las instrucciones para inscribirse en el programa de compras por volumen (VPP) en los dispositivos de la empresa antes de poder instalar aplicaciones de prepago. Los usuarios deben completar esta tarea una vez.

    Nota: Si concede acceso a un número de licencias superior al número de licencias disponibles, los primeros usuarios que accedan a las licencias disponibles podrán instalar la aplicación. Si la aplicación es una aplicación obligatoria que no tiene una licencia disponible, debe obtener la licencia antes de que el usuario pueda instalar la aplicación o dicho usuario estará sujeto a las reglas de cumplimiento que se hayan asignado al usuario.

Asignar una política de TI o un perfil a un grupo de dispositivos compartidos

Al asignar una política de Ti o un perfil a un grupo de dispositivos compartidos, estos se envían cuando un usuario desinscribe un dispositivo que está activado para el grupo y se eliminan cuando el usuario inscribe el dispositivo. Si desea que una política de TI o un perfil permanezca en los dispositivos cuando se inscriben, también debe asignarlos a la cuenta de usuario propietaria del grupo de dispositivos compartidos.

Antes de empezar:

- Si es necesario, Creación de una política de TI.
- Si fuera necesario, cree los perfiles. Para obtener más información, consulte Referencia de perfiles y Uso de variables en perfiles.

1. En la barra de menú, haga clic en **Usuarios > Dispositivos compartidos**.
2. Busque un grupo de dispositivos compartidos.
3. En los resultados de la búsqueda, haga clic en el nombre del grupo de dispositivos compartidos.
4. En la sección **Políticas de TI y perfiles asignados**, haga clic en +.
5. Haga clic en **Política de TI** o en un tipo de perfil.
6. En la lista desplegable, haga clic en el nombre de la política de TI o del perfil que desea asignar al grupo.
7. Lleve a cabo cualquiera de las tareas siguientes:

Tarea	Pasos
Asignar una política de TI	**a.** Si ya hay una política de TI asignada directamente al grupo, haga clic en **Sustituir**. De lo contrario, haga clic en **Asignar**.
Asignar un tipo de perfil clasificado	**a.** Si el tipo de perfil que ha seleccionado en el paso 5 ya está asignado directamente al grupo, haga clic en **Sustituir**. De lo contrario, haga clic en **Asignar**.
Asignar un tipo de perfil no clasificado	**a.** Haga clic en **Asignar**.

Creación de grupos de dispositivos

Un grupo de dispositivos es un conjunto de dispositivos con atributos comunes, tales como el modelo y el fabricante, el tipo y la versión del OS, el proveedor de servicios y si el dispositivo es propiedad de la empresa o del usuario. BlackBerry UEM mueve automáticamente los dispositivos dentro o fuera del grupo de dispositivos en función de los atributos que defina.

Puede utilizar grupos de dispositivos para aplicar diferentes conjuntos de políticas, de perfiles y de aplicaciones a los dispositivos asignados a un único usuario. Por ejemplo, puede utilizar un grupo de dispositivos para aplicar una política de TI específica a todos los dispositivos con BlackBerry 10 OS o a todos los dispositivos HTC EVO con Android OS versión 4.0 o una versión posterior en la red T-Mobile.

Las políticas, los perfiles y las aplicaciones asignadas a un grupo de dispositivos tienen prioridad sobre los asignados a un usuario o grupo de usuarios. Sin embargo, no puede asignar perfiles de activación o certificados de usuario a grupos de dispositivos.

Los grupos de dispositivos no incluyen los dispositivos con BlackBerry OS (de la versión 5.0 a la 7.1). Incluso si se crea una consulta de grupo de dispositivos que lógicamente incluiría los dispositivos con BlackBerry OS, estos no se incluyen en el grupo de dispositivos.

Creación de un grupo de dispositivos

1. En la barra de menú, haga clic en **Grupos > Dispositivo**.
2. Haga clic en .
3. Escriba un nombre para el grupo de dispositivos.
4. En la sección **Ámbito de los grupos de usuarios**, puede seleccionar uno o más grupos de usuarios para aplicar el grupo de dispositivos. Si no selecciona ninguno de los grupos de usuarios, el grupo de dispositivos se aplica a todos los dispositivos activados.
5. En la sección **Consulta de dispositivo**, en la primera lista desplegable, haga clic en **Cualquiera** o **Todo**.

   Si selecciona **Todo**, los dispositivos deben coincidir con todos los atributos que se definen para que se incluyan en el grupo de dispositivos. Si selecciona **Cualquiera**, los dispositivos tienen que coincidir únicamente con uno de los atributos que se definen para que se incluyan en el grupo de dispositivos.
6. En la sección **Consulta de dispositivo**, realice las acciones siguientes:
   - En la lista desplegable **Atributo**, haga clic en un atributo.
   - En la lista desplegable **Operador**, haga clic en un operador.
   - En la lista desplegable **Valor**, haga clic o escriba un valor.

   Puede agregar o eliminar filas para centrar su consulta.
7. Haga clic en **Next (Siguiente)**.
8. Para asignar una política de TI o un perfil al grupo de dispositivos, realice las siguientes acciones:
   a) En la sección **Política de TI y perfiles**, haga clic en +.
   b) Haga clic en **Política de TI** o en un tipo de perfil.
   c) En la lista desplegable, haga clic en el nombre de la política de TI o del perfil que desea asignar al grupo.
   d) Haga clic en **Asignar**.
9. Para asignar una aplicación o grupo de aplicaciones al grupo de dispositivos, en la sección **Aplicaciones asignadas**, haga clic en +.

   Nota: No puede agregar aplicaciones de BlackBerry Dynamics a grupos de dispositivos porque los derechos solo pueden otorgarse a los usuarios. Cualquier BlackBerry Dynamics incluido en los grupos de aplicaciones que agregue a los grupos de dispositivos no se asignará a los usuarios.

   Nota: No es posible agregar aplicaciones Android que tienen una disposición opcional a grupos de dispositivos en un entorno BlackBerry UEM que es compatible con perfiles de trabajo de Android. Google Play for Work no puede asignar aplicaciones a ID de dispositivo. Google Play for Work puede asignar aplicaciones únicamente a ID de usuario Google. Si agrega aplicaciones Android que tienen una disposición requerida a un grupo de dispositivos, las aplicaciones se instalarán, pero no se mostrarán en Google Play for Work.
10. Busque la aplicación.
11. En los resultados de la búsqueda, seleccione la aplicación.

12. Haga clic en **Next (Siguiente)**.
13. En la lista desplegable **Disposición** de la aplicación o del grupo de aplicaciones, realice una de las acciones siguientes:
    - Si la aplicación es una aplicación iOS o Android: para requerir a los usuarios a seguir las acciones definidas para las aplicaciones en el perfil de cumplimiento que se les asigna, seleccione **Obligatorio**.
    - Si la aplicación es un aplicación de Windows Phone:para instalar automáticamente una aplicación interna en dispositivos asignados, seleccione**Obligatorio**. Si los usuarios desinstalan la aplicación interna obligatoria, deben seguir las acciones definidas en el perfil de cumplimiento que se les asigna.Para las aplicaciones agregadas desde Windows Store, seleccione**Obligatorio**para que los usuarios deban seguir las acciones definidas para las aplicaciones en el perfil de cumplimiento que se les asigna. Se aplica únicamente a dispositivos con Windows Phone 8.1 o una versión posterior.
    - Si la aplicación es una aplicación de BlackBerry 10 interna: para instalar automáticamente una aplicación interna en dispositivos asignados, seleccione**Obligatorio**. El contenido solo está disponible para las aplicaciones de BlackBerry 10 internas. Las aplicaciones que se agregan de la tienda de BlackBerry World solo pueden ser opcionales.
    - Si el grupo de aplicaciones admite perfiles de trabajo de Android, la disposición solo se puede establecer como obligatoria.
    - Para permitir a los usuarios instalar y eliminar la aplicación, seleccione **Opcional**.

      Nota: La misma aplicación puede asignarse directamente a la cuenta de usuario o puede heredarse de grupos de usuarios o de dispositivos. La configuración de la aplicación (por ejemplo, si la aplicación es obligatoria) se asigna en función de la prioridad: los grupos de dispositivos tienen prioridad sobre las cuentas y los grupos de usuarios.
14. En los dispositivos iOS, para asignar los ajustes de VPN por aplicación a una aplicación o grupo de aplicaciones, en la lista desplegable **VPN por aplicación** para la aplicación o grupo de aplicaciones, seleccione los ajustes que desea asociar a la aplicación o grupo de aplicaciones.
15. Para dispositivos iOS y Android, si hay disponible una configuración de aplicaciones, seleccione la configuración de aplicaciones que desee asignar a la aplicación.
16. Haga clic en **Asignar**.
17. Cuando termine de especificar las propiedades del grupo de dispositivos, haga clic en **Guardar**.

Edite un grupo de dispositivos

1. En la barra de menú, haga clic en **Grupos > Dispositivo**.
2. Haga clic en el nombre del grupo de dispositivos que desee editar.
3. Haga clic en ✎.
4. Realice las ediciones necesarias.
5. Haga clic en **Guardar**.

Definición de parámetros de grupos de dispositivos

Cuando se crea un grupo de dispositivos, se configura una consulta de dispositivo que incluye una o más instrucciones de atributo. Puede especificar si un dispositivo pertenece al grupo de dispositivos, si coincide con cualquier instrucción de atributo o solo si coincide con todas las instrucciones de atributo. Cada instrucción de atributo contiene un atributo, un operador y un valor.

Atributo	Operadores	Valores
Operador	• = • != • Comienza por	En el campo de texto, escriba el nombre de un proveedor de servicios, como T-Mobile o Bell.
Con BlackBerry Dynamics	• = • !=	En la lista desplegable, seleccione una de las opciones siguientes: • Desactivado • Activado
Fabricante	• = • != • Comienza por	En el campo de texto, escriba el nombre de un fabricante del dispositivo, como Apple o BlackBerry.
Modelo	• = • != • Comienza por	En el campo de texto, escriba el nombre de un modelo de dispositivo, como iPhone 5S o BlackBerry Classic.
SO	• = • !=	En la lista desplegable, seleccione una de las opciones siguientes: • Android • BlackBerry 10 • iOS • Windows
Versión del SO	• = • != • >= • <=	En el campo de texto, escriba una versión del SO, como 7.1.1 o 10.3. Si se utiliza este atributo, también deberá especificar el atributo del SO.
Propiedad	• = • !=	En la lista desplegable, seleccione una de las opciones siguientes: • Trabajo • Personal • No especificado
Tipo de activación	• = • !=	En la lista desplegable, seleccione un tipo de activación. La lista contiene los mismos tipos de activación que están disponibles para su asignación en los perfiles de activación.
KNOX Workspace	• = • != • Comienza por	En el campo de texto, escriba una versión de Samsung KNOX Workspace como 2.2.

Presentación de un grupo de dispositivos

1. En la barra de menú, haga clic en **Grupos > Dispositivos**.

2. Busque el grupo de dispositivos que desea ver.
3. Haga clic en el grupo de dispositivos.
4. Lleve a cabo una de las siguientes acciones:
   - Para ver los dispositivos asignados al grupo de dispositivos, haga clic en la pestaña **Dispositivos**.
   - Para ver los grupos de usuarios, las consultas de los dispositivos, las políticas de TI, los perfiles o las aplicaciones asignadas al grupo de dispositivos, seleccione la pestaña **Ajustes**.

Cambie el nombre de un grupo de dispositivos

1. En la barra de menú, haga clic en **Grupos > Dispositivo**.
2. Busque el grupo de dispositivos que desea ver.
3. Haga clic en el grupo de dispositivos.
4. Haga clic en .
5. Cambie el nombre del grupo de dispositivos.
6. Haga clic en **Siguiente**.
7. Haga clic en **Guardar**.

Eliminar un grupo de dispositivos

Para poder eliminar un grupo de dispositivos, debe tener permiso para administrar todos los grupos de usuarios a los que se ha aplicado el grupo de dispositivos.

1. En la barra de menú, haga clic en **Grupos > Dispositivo**.
2. Busque el grupo de dispositivos que desea ver.
3. Haga clic en el grupo de dispositivos.
4. Haga clic en .
5. Haga clic en **Eliminar**.

Presentación y personalización de la lista de usuarios

Puede ver y personalizar la lista de usuarios mediante la configuración de la vista predeterminada o avanzada y, a continuación, seleccionar la información que desea que se muestre en la lista de usuarios. Puede seleccionar y volver a ordenar las columnas de la lista de usuarios, ya que existen más columnas disponibles en la vista avanzada.

Puede utilizar filtros para ver únicamente la información relevante para su tarea. Puede filtrar la lista de usuarios mediante la selección de un filtro cada vez o la selección de varios filtros. En la vista predeterminada, puede filtrar la lista de usuarios por SO, proveedor de servicios inalámbricos, grupo, política de TI asignada, propiedad e infracción del cumplimiento. En la vista avanzada existen más categorías disponibles. Por ejemplo, puede filtrar la lista de usuarios por modelo, versión de SO y el tipo de activación.

Para el análisis más detallado o para la generación de informes, puede exportar la lista de usuarios a un archivo .csv.

Establezca la vista predeterminada o avanzada

Puede establecer la vista que utiliza el navegador para mostrar la lista de usuarios de BlackBerry UEM. En la vista avanzada existen más categorías de columnas y de filtros disponibles.

Nota: En entornos de mayor tamaño, la vista avanzada puede tardar más tiempo en mostrarse que la vista predeterminada.

1. En la barra de menú, haga clic en **Usuarios > Dispositivos gestionados**.
2. En la esquina superior derecha, haga clic en **Predeterminado** o **Avanzado**.

Después de terminar: Seleccione la información que desea que aparezca en la lista de usuarios.

Seleccione la información que desea que aparezca en la lista de usuarios

Antes de empezar: Establezca la vista predeterminada o avanzada.

1. En la barra de menú, haga clic en **Usuarios > Dispositivos gestionados**.
2. Haga clic en + en la parte superior de la lista de usuarios y realice cualquiera de las siguientes acciones:
   - Haga clic en **Seleccionar todo** o seleccione la casilla de verificación correspondiente a cada columna que desee mostrar.
   - Desactive la casilla de verificación correspondiente a cada una de las columnas que desea eliminar.
   - Haga clic en **Restablecer** para volver a las selecciones predeterminadas.
3. Para clasificar la lista de usuarios, haga clic en el encabezado de una columna.
4. Para volver a ordenar las columnas, haga clic en el encabezado de una columna y arrástrelo hacia la izquierda o la derecha.

Filtrado de la lista de usuarios

Al activar la selección múltiple, puede seleccionar varios filtros antes de aplicarlos y también seleccionar varios filtros en cada categoría. Si desactiva la selección múltiple, cada filtro se aplicará cuando lo seleccione y solo puede seleccionar un filtro en cada categoría.

Antes de empezar: Establezca la vista predeterminada o avanzada.

1. En la barra de menú, haga clic en **Usuarios**.
2. Haga clic en para activar o desactivar la selección múltiple.
3. En **Filtros**, amplíe una o más categorías.

   Cada categoría incluye solo los filtros que muestran resultados y cada filtro indica el número de resultados que se mostrarán al aplicarlo.
4. Lleve a cabo una de las siguientes acciones:
   - Si activó la selección múltiple, seleccione la casilla de verificación de cada filtro que desea aplicar y haga clic en **Enviar**.
   - Si desactivó la selección múltiple, haga clic en el filtro que desea aplicar.
5. De forma opcional, en el panel derecho, haga clic en **Borrar todo** o en × para cada filtro que desee eliminar.

Clasificación de la lista de usuarios

Puede clasificar la lista de usuarios alfabéticamente por cualquiera de las categorías que se muestran en los encabezados de columna.

Antes de empezar: Establezca la vista predeterminada o avanzada.

1. En la barra de menú, haga clic en **Usuarios** y seleccione la pestaña que quiere ver.
2. Si fuera necesario, filtre la lista de usuarios.
3. Toque el encabezado de una columna. Haga clic en la encabezado de columna de nuevo para clasificar en orden inverso.

Exportación de la lista de usuarios a un archivo .csv

Al exportar la lista de usuarios a un archivo .csv, dicho archivo incluirá todas las columnas disponibles en la vista predeterminada o avanzada.

Antes de empezar: Establezca la vista predeterminada o avanzada.

1. En la barra de menú, haga clic en **Usuarios > Dispositivos gestionados**.
2. Si fuera necesario, filtre la lista de usuarios.
3. Lleve a cabo una de las siguientes acciones:
   - Seleccione la casilla de verificación en la parte superior de la lista de usuarios para seleccionar todos los usuarios.
   - Seleccione la casilla de verificación de cada usuario que desee incluir en el archivo. Puede utilizar Mayús +clic para seleccionar varios usuarios.
4. Haga clic en y guarde el archivo.

Tareas relacionadas

Filtrado de la lista de usuarios

Cambio de la etiqueta de la propiedad de dispositivo

Cada dispositivo activado en BlackBerry UEM tiene una etiqueta que indica si el dispositivo es propiedad de su empresa o del usuario, o si no se ha especificado. El valor predeterminado para esta etiqueta proviene de la configuración de propiedad del dispositivo en el perfil de activación. Puede editar la etiqueta de propiedad en cualquier momento. Para cambiar esta configuración para varios dispositivos de una vez, consulte Envío de un comando masivo.

La etiqueta de propiedad del dispositivo es útil si desea filtrar la lista de usuarios con la configuración de propiedad del dispositivo. Para obtener más información, consulte Filtrado de la lista de usuarios.

1. En la barra de menú, haga clic en **Usuarios > Dispositivos gestionados**.
2. Busque una cuenta de usuario.
3. En los resultados de la búsqueda, haga clic en el nombre de la cuenta de usuario.
4. Haga clic en la pestaña del dispositivo.
5. En la sección de dispositivo activado, junto a la configuración de propiedad, haga clic en **Editar**.
6. En la lista desplegable, seleccione una de las opciones siguientes:
   - Trabajo
   - Personal
   - No especificado
7. Haga clic en **Guardar**.

Activación del dispositivo

Cuando active un dispositivo, podrá asociarlo a BlackBerry UEM de modo que pueda administrar dispositivos y que los usuarios puedan acceder a los datos de trabajo en sus dispositivos.

Al activar un dispositivo, puede enviar las políticas de TI y los perfiles para controlar las características disponibles y administrar la seguridad de los datos de trabajo. También puede asignar aplicaciones para que el usuario las instale. En función del nivel de control que el tipo de activación seleccionado permita, también podrá proteger el dispositivo mediante la restricción del acceso a determinados datos, la configuración de contraseñas de forma remota, el bloqueo del dispositivo o la eliminación de datos.

Puede asignar distintos tipos de activación para adaptarse a los requisitos de los dispositivos que son propiedad de la empresa y los dispositivos que son propiedad de los usuarios. Los distintos tipos de activación le ofrecen distintos grados de control sobre los datos de trabajo y los datos personales en los dispositivos, que van desde el total control sobre todos los datos al control específico únicamente de los datos de trabajo.

Pasos para activar los dispositivos

Al activar dispositivos, realice las acciones siguientes.

Paso	Acción
1	Compruebe que se cumplan todos los requisitos de activación.
2	Configure la configuración de activación predeterminada.
3	Si procede, revise la siguiente información: • Si tiene previsto admitir dispositivos Android que utilizan un perfil de trabajo, consulte Soporte de activaciones para dispositivos Android con un perfil de trabajo. • Si tiene pensado admitir dispositivos Windows 10, consulte Compatibilidad con las activaciones de Windows 10 .
4	Actualice la plantilla para el correo de activación.
5	Cree un perfil de activación y asígnelo a una cuenta de usuario o a un grupo al que pertenezca el usuario.
6	Establezca una contraseña de activación para el usuario.

Requisitos: activación

Para todos los dispositivos:

- Una licencia disponible en BlackBerry UEM para el dispositivo que desea activar. Para obtener más información acerca de las licencias, consulte el contenido referente a licencias.
- Una conexión inalámbrica que funcione

Para los dispositivos iOS, Android y Windows Phone 8.0 y 8.1:

- La última versión de la aplicación BlackBerry UEM Client instalada en el dispositivo

Para dispositivos Windows 10 y Windows 10 Mobile:

- Un certificado de BlackBerry Enterprise Server raíz de RSA instalado en el dispositivo
- Para dispositivos que utilizan una configuración de proxy, un proxy que no requiera autenticación. Para obtener más información, consulte https://docs.microsoft.com/en-us/windows/client-management/mdm/new-in-windows-mdm-enrollment-management
- Para ordenadores, Windows 10 Home solo ofrece compatibilidad limitada.

Para "Solo espacio de trabajo" en dispositivos Android que tengan un perfil de trabajo:

- Un código de activación de Google

Para dispositivos con BlackBerry OS (de la versión 5.0 a 7.1):

- Una cuenta de usuario en un directorio en el servidor de correo de trabajo con la que el servidor de correo de BlackBerry OS se conecta
- La activación del dispositivo con BlackBerry OS activada para la cuenta de usuario

Nota: Puede verse un vídeo sobre cómo activar el dispositivo aquí: http://help.blackberry.com/detectLang/activation-videos/current/

Gestión de las contraseñas de activación

Puede tener cierto control sobre el número de dispositivos que pueden activar los usuarios mediante la gestión de las contraseñas de activación que se envían a los usuarios.

A continuación, se muestran ejemplos de cómo puede gestionar las contraseñas de activación:

- Cuando configura contraseñas de activación para los usuarios, puede hacer lo siguiente:
  - Hacer que BlackBerry UEM genere automáticamente una contraseña de activación o puede especificar una contraseña de activación.
  - Especificar durante cuánto tiempo es válida la contraseña de activación (en minutos o días).
  - Especificar que el periodo de activación caduque en cuanto el usuario active un dispositivo, lo que limita de manera eficaz el número de dispositivos que el usuario puede activar con esa contraseña a uno.

  Para obtener más información, consulte Establezca una contraseña de activación y envíe un mensaje de correo de activación.
- Puede crear varias contraseñas para un usuario y emparejar las contraseñas con perfiles de activación específicos. Para obtener más información, consulte Permitir que los usuarios activen varios dispositivos con diferentes tipos de activación.
- Si permite a los usuarios configurar contraseñas de activación en BlackBerry UEM Self-Service, los usuarios pueden crear contraseñas de activación cuando sea necesario, pero solo pueden activar el número de dispositivos especificado en el perfil de la activación. Para obtener más información, consulte Autorización a usuarios para configurar contraseñas de activación en BlackBerry UEM Self-Service.
- Puede hacer que las contraseñas de activación caduquen para un usuario en cualquier momento. Para obtener más información, consulte Hacer caducar manualmente una contraseña de activación.
- Si va a implementar dispositivos con Samsung KNOX Mobile Enrollment, puede permitir a los usuarios de esos dispositivos que utilicen sus credenciales de Microsoft Active Directory para activar sus dispositivos. En

lugar de gestionar las contraseñas de activación de cada usuario, puede indicar a los usuarios que utilicen sus credenciales de Active Directory. Esta opción se aplica únicamente a los dispositivos inscritos en la cuenta de KNOX Mobile Enrollment de su empresa. Para obtener más información, consulte Especificación de la configuración predeterminada para las contraseñas de activación.

Especificación de la configuración predeterminada para las contraseñas de activación

Puede especificar el tiempo predeterminado que una contraseña de activación es válida antes de que caduque. También puede especificar la longitud de las contraseñas generadas automáticamente que se envían a los usuarios en uno de los mensajes de correo de activación y si desea o no que el periodo de activación caduque después de que se active el primer dispositivo.

El valor que introduzca para la caducidad de la contraseña de activación aparece como la configuración predeterminada en el campo Caducidad de la contraseña de activación en las ventanas Establecer contraseña de activación del dispositivo y Agregar un usuario.

Para los dispositivos activados mediante Samsung KNOX Mobile Enrollment, también puede especificar si se permite a los usuarios utilizar sus credenciales de Microsoft Active Directory para activar sus dispositivos.

1. En la barra de menús, haga clic en **Configuración**.
2. En el panel izquierdo, amplíe **Configuración general**.
3. Haga clic en **Activación predeterminada**.
4. En el campo **Caducidad del periodo de activación**, introduzca el tiempo predeterminado durante el que una contraseña de activación (o QR Code) es válida antes de que caduque. El tiempo puede estar oscilar entre 1 minuto y 30 días.
5. Si es necesario, seleccione la casilla de verificación **El periodo de activación caduca después de la activación del primer dispositivo**.
6. Seleccione o anule la selección de la casilla de verificación **Permitir códigos QR para la activación de dispositivos**. Si esta opción está seleccionada, puede elegir enviar QR Code a los usuarios en lugar de una contraseña de activación. Si no selecciona esta opción, la opción de enviar QR Code no está disponible en la plantilla del correo de activación.
7. Si es necesario, para los dispositivos activados mediante KNOX Mobile Enrollment, seleccione **Permitir el uso del nombre de usuario y la contraseña de Microsoft Active Directory**.
8. Seleccione o anule la selección de la casilla de verificación **Enviar notificación de dispositivo activado**. Si se selecciona, el usuario recibe un mensaje de correo electrónico cuando se activa un dispositivo.
9. En el campo **Longitud de la contraseña de activación generada automáticamente**, especifique la longitud de la contraseña de activación generada automáticamente. El valor puede oscilar entre 4 y 16.
10. En la sección **Complejidad de la contraseña generada automáticamente**, seleccione una o más de las opciones siguientes:
    - Letras minúsculas
    - Letras mayúsculas
    - Números
    - Caracteres especiales o símbolos
11. Seleccione o anule la selección de la casilla de verificación **Activar registro con BlackBerry Infrastructure** para modificar la forma en que los usuarios activan los dispositivos móviles. Si no selecciona esta opción, los usuarios deberán proporcionar la dirección del servidor para BlackBerry UEM al activar dispositivos. Para obtener más información, consulte Activación del registro de usuario con BlackBerry Infrastructure.
12. Haga clic en **Guardar**.

Permitir que los usuarios activen varios dispositivos con diferentes tipos de activación

Puede crear varias contraseñas de activación para un usuario y emparejar las contraseñas de activación con perfiles de activación específicos de modo que los usuarios puedan activar los dispositivos con diferentes tipos de activación.

Por ejemplo, es posible que desee que los usuarios activen dispositivos de trabajo con un tipo de activación que le permita tener control total de los dispositivos y que activen sus dispositivos personales con un tipo de activación que permita la privacidad del usuario. Mediante el emparejamiento de una contraseña de activación con un perfil de activación que permite el control total de los dispositivos y una segunda contraseña de activación con el perfil de activación de privacidad de usuario, los usuarios pueden activar cada dispositivo con diferentes resultados. Puede crear plantillas de correo que describan el uso previsto para cada contraseña.

Seleccione la opción "Activación del dispositivo con perfil de activación especificado" cuando realice cualquiera de las siguientes tareas:

- Creación de una cuenta de usuario
- Establezca una contraseña de activación y envíe un mensaje de correo de activación
- Envío de un mensaje de correo electrónico de activación a varios usuarios

En un momento dado, puede tener un máximo de dos contraseñas de activación emparejadas con perfiles de activación específicos. Cada contraseña se puede usar para activar varios dispositivos.

Nota: Para las contraseñas de activación que están emparejadas con perfiles de activación específicos, la configuración "Número de dispositivos que un usuario puede activar" en el perfil de activación no se aplica.

Si elimina un perfil de activación emparejado con una contraseña de activación, dicha contraseña caduca automáticamente.

Si es necesario, puede hacer que las contraseñas de activación caduquen para un usuario en particular en cualquier momento. Para obtener más información, consulte Hacer caducar manualmente una contraseña de activación.

A diferencia de las contraseñas de activación normales, los usuarios no pueden crear contraseñas de activación que se emparejan con perfiles de activación específicos en BlackBerry UEM Self-Service.

Esta opción no es compatible con dispositivos iOS inscritos en DEP.

Hacer caducar manualmente una contraseña de activación

Puede hacer caducar manualmente una contraseña de activación que se generó para un usuario.

1. En la barra de menú, haga clic en **Usuarios > Dispositivos gestionados**.
2. Busque una cuenta de usuario.
3. En los resultados de la búsqueda, haga clic en el nombre de la cuenta de usuario.
4. En la sección **Detalles de activación**, localice la contraseña de activación que desea que caduque. Haga clic en **Caducar**. La contraseña de activación caduca inmediatamente.

   Si hace caducar una contraseña de activación normal, se muestra la fecha y la hora en la que la contraseña caduca.

   Si hace caducar una contraseña de activación que se emparejó con un perfil de activación específico, los detalles de la contraseña de activación del dispositivo ya no se muestran.

Establezca una contraseña de activación y envíe un mensaje de correo de activación

Puede establecer una contraseña de activación y enviar un correo de activación a un usuario con la información necesaria para activar uno o más dispositivos.

El correo se envía desde la dirección de correo que haya configurado en la configuración del servidor SMTP.

Antes de empezar: Creación de una plantilla de correo de activación.

1. En la barra de menú, haga clic en **Usuarios > Dispositivos gestionados**.
2. Busque una cuenta de usuario.
3. En los resultados de la búsqueda, haga clic en el nombre de la cuenta de usuario.
4. En el panel de Detalles de activación, haga clic en **Establecer contraseña de activación**.
5. En la lista desplegable **Opción de activación**, lleve a cabo una de las tareas siguientes:
   - Si desea que el usuario pueda activar su dispositivo con el perfil de activación que tiene actualmente asignado, seleccione **Activación del dispositivo predeterminada**. Puede ver el perfil de activación que se asigna al usuario en la sección Política de TI y perfiles en la pestaña Resumen.
   - Si desea emparejar una contraseña de activación con un perfil de activación específico, seleccione **Activación del dispositivo con perfil de activación especificado**. Para obtener más información, consulte Permitir que los usuarios activen varios dispositivos con diferentes tipos de activación.
6. En la lista desplegable **Contraseña de activación**, realice una de las tareas siguientes:
   - Si desea generar automáticamente una contraseña, seleccione **Generar automáticamente la contraseña de activación del dispositivo y enviar un correo electrónico con las instrucciones de activación**. Cuando se selecciona esta opción, deberá seleccionar una plantilla de correo para enviar la información al usuario.
   - Si desea establecer una contraseña de activación para el usuario y, opcionalmente, enviar un correo electrónico de activación, seleccione **Establecer contraseña de activación del dispositivo**.
7. De manera opcional, puede cambiar la caducidad del periodo de activación. La caducidad del periodo de activación especifica cuánto tiempo la contraseña de activación sigue siendo válida.
8. Si desea que la contraseña de activación sea válida solo para una activación de dispositivo, seleccione **El periodo de activación caduca después de la activación del primer dispositivo**.
9. En la lista desplegable **Plantilla del correo de activación**, seleccione la plantilla de correo que desea usar. Para obtener más información, consulte Plantillas de correo.
10. Haga clic en **Enviar**.

Envío de un mensaje de correo electrónico de activación a varios usuarios

Puede enviar mensajes de correo de activación a varios usuarios al mismo tiempo. Cuando envíe un mensaje de correo electrónico de activación a varios usuarios, la contraseña de activación se generará automáticamente. Si desea establecer la contraseña de activación, consulte Establezca una contraseña de activación y envíe un mensaje de correo de activación.

El correo se envía desde la dirección de correo que haya configurado en la configuración del servidor SMTP.

Antes de empezar: Creación de una plantilla de correo de activación.

1. En la barra de menú, haga clic en **Usuarios > Dispositivos gestionados**.
2. Seleccione la casilla de verificación para cada usuario al que desee enviar un mensaje de correo electrónico de activación.
3. Haga clic en .
4. En la lista desplegable **Opción de activación**, lleve a cabo una de las tareas siguientes:
   - Si desea que los usuarios puedan activar sus dispositivos con el perfil de activación que tienen actualmente asignado, seleccione **Activación del dispositivo predeterminada**.
   - Si desea emparejar una contraseña de activación con un perfil de activación específico, seleccione **Activación del dispositivo con perfil de activación especificado**. Para obtener más información acerca del emparejamiento de contraseñas de activación con perfiles de activación, consulte Permitir que los usuarios activen varios dispositivos con diferentes tipos de activación.
5. En la lista desplegable **Contraseña de activación**, seleccione **Generar automáticamente la contraseña de activación del dispositivo y enviar un correo electrónico con las instrucciones de activación**.

6. De manera opcional, puede cambiar la caducidad del periodo de activación. La caducidad del periodo de activación especifica cuánto tiempo la contraseña de activación sigue siendo válida.
7. Si desea que la contraseña de activación sea válida solo para una activación de dispositivo, seleccione **El periodo de activación caduca después de la activación del primer dispositivo**.
8. En la lista desplegable **Plantilla del correo de activación**, seleccione la plantilla de correo que desea usar. Para obtener más información, consulte Plantillas de correo.
9. Haga clic en **Enviar**.

Autorización a usuarios para configurar contraseñas de activación en BlackBerry UEM Self-Service

Puede permitir a los usuarios con dispositivos BlackBerry 10, iOS, Android y Windows crear sus propias contraseñas de activación mediante BlackBerry UEM Self-Service.

Nota: Los usuarios de dispositivos con BlackBerry OS (versión 5.0 a 7.1) pueden crear contraseñas de activación mediante BlackBerry Web Desktop Manager.

1. En la barra de menú, haga clic en **Configuración > Configuración general > Autoservicio**.
2. Compruebe que **Permitir que los usuarios accedan a la consola de autoservicio** está seleccionado.
3. Seleccione **Permitir que los usuarios activen los dispositivos a través de la consola de autoservicio** y complete las siguientes tareas:
   a) Especifique el número de minutos, las horas o los días en los que un usuario puede activar un dispositivo antes de que caduque la contraseña de activación.
   b) Especifique el número mínimo de caracteres requeridos en una contraseña de activación.
   c) En la lista desplegable **Complejidad mínima de la contraseña**, seleccione el nivel de complejidad requerido para contraseñas de activación.
4. Haga clic en **Guardar**.

Activación del registro de usuario con BlackBerry Infrastructure

El registro con BlackBerry Infrastructure simplifica la forma en que los usuarios activan sus dispositivos móviles. Con el registro activado, los usuarios no necesitan introducir la dirección del servidor cuando activan los dispositivos. El registro está activado de forma predeterminada. Si cambia este ajuste, tal vez necesite actualizar el correo de activación con los pasos que los usuarios deben realizar para activar sus dispositivos.

Los dispositivos que ejecutan Windows 10 y Windows 10 Mobile no utilizan el mismo método para ponerse en contacto con BlackBerry Infrastructure, de modo que activar o desactivar el registro de usuarios no cambia el proceso de activación para estos dispositivos.

Los dispositivos que ejecutan BlackBerry OS (de la versión 5.0 a la 7.1) no establecen contacto con BlackBerry Infrastructure, de modo que activar o desactivar el registro de usuarios no cambia el proceso de activación para estos dispositivos.

1. En la barra de menús, haga clic en **Configuración**.
2. En el panel izquierdo, amplíe **Configuración general**.
3. Haga clic en **Activación predeterminada**.
4. Asegúrese de que la casilla de verificación **Activar registro con BlackBerry Infrastructure** está seleccionada.
5. Haga clic en **Guardar**.

Habilitar la notificación al usuario cuando se ha activado un dispositivo

Puede activar UEM para que notifique a un usuario cada vez que se activa un dispositivo en su cuenta. La notificación por correo electrónico se envía a la dirección de correo electrónico de la cuenta del usuario que se utilizó para activar el dispositivo. De forma predeterminada, el correo electrónico incluye el modelo de dispositivo, el número de serie y el IMEI. Si el usuario recibe una notificación que no esperaba, debe ponerse en contacto con un administrador.

1. En la barra de menú, haga clic en **Configuración** > **Configuración general**.
2. Haga clic en **Activación predeterminada**.
3. Seleccione **Enviar notificación de dispositivo activado**.
4. Haga clic en **Guardar**.

Tareas relacionadas

Edición de una plantilla de correo

Referencia relacionada

Plantillas de correo predeterminadas
Texto sugerido

Soporte de activaciones para dispositivos Android con un perfil de trabajo

Para respaldar activaciones de dispositivos Android con un perfil de trabajo, realice las siguientes tareas según sea necesario:

- Si tiene un dominio G Suite consulte Es compatible con las activaciones de perfiles de trabajo de Android con un dominio G Suite.
- Si tiene un dominio Google Cloud consulte Es compatible con las activaciones de perfiles de trabajo de Android con un dominio Google Cloud.
- Compruebe que BlackBerry Hub funcionará correctamente en dispositivos Android con un perfil de trabajo. Consulte Activación de un BlackBerry Hub unificado.

Es compatible con las activaciones de perfiles de trabajo de Android con un dominio G Suite

Si ha configurado BlackBerry UEM para conectarse a un dominio de G Suite, debe realizar las siguientes tareas antes de que los usuarios puedan activar los dispositivos Android que tengan un perfil de trabajo.

Antes de empezar: Configure BlackBerry UEM para que admita dispositivos Android con un perfil de trabajo. Para obtener información sobre la configuración de BlackBerry UEM para admitir Android con un perfil de trabajo, consulte el contenido de Configuración.

1. En el dominio de G Suite, cree cuentas de usuario para los usuarios de Android.
2. Si los usuarios tienen dispositivos con Android versión 6.0 o posterior, seleccione la configuración **Aplicar política de EMM** en el dominio G Suite.

Esta configuración es necesaria para dispositivos con el tipo de activación Solo espacio de trabajo y se recomienda encarecidamente para dispositivos con otros tipos de activación. Si esta configuración no se selecciona, los usuarios pueden agregar una cuenta de Google gestionada al dispositivo que pude acceder a las aplicaciones de trabajo fuera del perfil de trabajo.

3. Si desea asignar el tipo de activación Solo espacio de trabajo y algunos usuarios tienen dispositivos con Android 6.0 o posterior, seleccione la configuración **Aplicar política de EMM** en el dominio de G Suite.
4. En BlackBerry UEM, cree cuentas de usuario locales para los usuarios de Android. La dirección de correo de cada cuenta debe coincidir con la dirección de correo de la cuenta de G Suite correspondiente.
5. Asegúrese de que los usuarios conozcan las contraseñas de las cuentas de G Suite.
6. En BlackBerry UEM, asigne un perfil de correo electrónico y aplicaciones de productividad a los usuarios, grupos de usuarios o grupos de dispositivos.

Es compatible con las activaciones de perfiles de trabajo de Android con un dominio Google Cloud

Si ha configurado BlackBerry UEM para conectarse a un dominio de Google Cloud, debe realizar las siguientes tareas antes de que los usuarios puedan activar los dispositivos mediante perfiles de trabajo de Android.

Antes de empezar: Configure BlackBerry UEM para que sea compatible con perfiles de trabajo de Android. Cuando se configura BlackBerry UEM para conectarse a un dominio de Google Cloud, debe seleccionar si BlackBerry UEM puede crear cuentas de usuario en el dominio. Esta selección afecta a las tareas que se deben realizar antes de que los usuarios pueden activar los dispositivos con Android que tienen un perfil de trabajo. Para obtener información sobre la configuración de BlackBerry UEM para admitir dispositivos Android que tienen un perfil de trabajo, consulte el contenido de Configuración.

1. En BlackBerry UEM, agregue las cuentas de usuario del directorio para los usuarios de perfil de trabajo de Android.
2. Si elige no permitir a BlackBerry UEM crear cuentas de usuario en el dominio de Google Cloud, deberá crear cuentas de usuario en el dominio de Google Cloud y en BlackBerry UEM. Lleve a cabo una de las siguientes acciones:
   - En el dominio de Google Cloud, cree cuentas de usuario para los usuarios de perfil de trabajo de Android. Cada dirección de correo debe coincidir con la dirección de correo de la cuenta de usuario de BlackBerry UEM correspondiente. Asegúrese de que los usuarios del perfil de trabajo de Android conozcan la contraseña de las cuentas de Google Cloud.
   - Utilice Google Apps Directory Sync Tool para sincronizar el dominio de Google Cloud con el directorio de la empresa. Si lo hace, no tendrá que crear manualmente las cuentas de usuario en el dominio de Google Cloud.
3. Si desea asignar el tipo de activación Solo espacio de trabajo y algunos usuarios tienen dispositivos con Android 6.0 o posterior, seleccione la configuración **Aplicar política de EMM** en el dominio de Google Cloud.
4. En BlackBerry UEM, asigne un perfil de correo electrónico y aplicaciones de productividad a los usuarios, grupos de usuarios o grupos de dispositivos.

Activación de un BlackBerry Hub unificado

BlackBerry Hub es una aplicación que permite a los usuarios ver los mensajes, las notificaciones y los eventos en un solo lugar.

Para permitir que los usuarios con dispositivos con Android Enterprise puedan ver tanto los mensajes personales como los de trabajo en BlackBerry Hub, es necesario verificar algunos ajustes en BlackBerry UEM.

1. Para la política de TI asignada a los usuarios, en la sección BlackBerry Productivity Suite, verifique que la regla de política de TI "Permitir vista de cuentas unificada en BlackBerry Hub" está seleccionada.
2. Lleve a cabo una de las tareas siguientes:

- Si configura los ajustes para BlackBerry Hub en un perfil de correo, en la pestaña Android del perfil de correo, verifique que los siguientes elementos están seleccionados:
  - Permitir el uso compartido de datos entre perfiles personales y de trabajo
  - Permitir que las aplicaciones personales accedan a los datos de trabajo
- Si configura los ajustes para BlackBerry Hub en la configuración de una aplicación, verifique que los siguientes elementos están seleccionados:
  - IPC entre perfiles
  - Acceder al contenido de trabajo

Después de terminar:

Para obtener información acerca del uso de BlackBerry Hub en dispositivos, como agregar una cuenta de correo electrónico o personalizar la configuración de BlackBerry Hub, consulte el contenido de BlackBerry Hub.

Para obtener información sobre la resolución de problemas, visite http://support.blackberry.com/kb y lea el artículo 37721.

Compatibilidad con las activaciones de Windows 10

Puede ayudar a los usuarios a activar los dispositivos con Windows 10 de dos formas:

- Implemente un servicio de detección para simplificar las activaciones de Windows 10. Para obtener más información, consulte el contenido de Configuración.
- Cree o edite una plantilla de correo de activación para proporcionar la información de activación de Windows 10. Para obtener más información, consulte "Creación de una plantilla de correo de activación ".

Creación de perfiles de activación

Puede controlar el modo en que los dispositivos se activan y se gestionan mediante perfiles de activación. Un perfil de activación especifica cuántos y qué tipos de dispositivos puede activar un usuario y el tipo de activación para cada tipo de dispositivo.

El tipo de activación le permite configurar el nivel de control que tiene sobre los dispositivos activados. Es posible que desee tener el control total sobre un dispositivo que entrega a un usuario. Es posible que deba asegurarse de no tener ningún control sobre los datos personales en un dispositivo que un usuario posee y que lleva al trabajo.

El perfil de activación asignado se aplica solo a los dispositivos que el usuario activa después de que se asigne el perfil. Los dispositivos que ya están activados no se actualizan automáticamente para que coincida con el perfil de activación nuevo o actualizado.

Cuando se agrega un usuario a BlackBerry UEM, el perfil de activación predeterminado se asigna a la cuenta de usuario. Puede cambiar el perfil de activación predeterminado para satisfacer sus necesidades, o puede crear un perfil de activación personalizado y asignarlo a los usuarios o a los grupos de usuarios.

Los perfiles de activación no se aplican a los dispositivos BlackBerry OS (de la versión 5.0 a la 7.1).

Creación de un perfil de activación

1. En la barra de menú, haga clic en **Políticas y perfiles**.
2. Haga clic en **Política > Activación**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil.

5. En el campo **Número de dispositivos que un usuario puede activar**, especifique el número máximo de dispositivos que el usuario puede activar.
6. En la lista desplegable **Propiedad del dispositivo**, seleccione la configuración predeterminada para la propiedad del dispositivo. Lleve a cabo una de las siguientes acciones:
   - Si algunos usuarios activan dispositivos personales y algunos usuarios activan los dispositivos de trabajo, seleccione **No especificado**.
   - Si los usuarios suelen activar los dispositivos de trabajo, seleccione **Trabajo**.
   - Si los usuarios suelen activar dispositivos personales, seleccione **Personal**.
7. Opcionalmente, seleccione un aviso de la empresa en la lista desplegable **Asignar aviso de la organización**. Si asigna un aviso de la empresa, los usuarios que activen los dispositivos con BlackBerry 10, Windows 10, iOS o macOS deberán aceptar el aviso para completar el proceso de activación.
8. En la sección **Tipos de dispositivo que los usuarios pueden activar**, seleccione los tipos de dispositivo según sea necesario. Los tipos de dispositivo que no seleccione no se incluirán en el perfil de activación y los usuarios no podrán activar dichos dispositivos.
9. Realice las siguientes acciones para cada tipo de dispositivo incluido en el perfil de activación:
   - Haga clic en la pestaña del tipo de dispositivo.
   - En la lista desplegable **Restricciones de modelo de dispositivo**, seleccione si desea permitir o restringir los dispositivos especificados o no aplicar restricciones. Haga clic en **Editar** para seleccionar los dispositivos que desee restringir o permitir y, a continuación, haga clic en **Guardar**.
   - En la lista desplegable **Versión permitida**, seleccione la versión mínima permitida.
   - En la pestaña **Windows**, puede seleccionar una o ambas opciones de factor de forma y elegir si desea permitir dichos factores de forma en la lista desplegable **Restricciones de modelo de dispositivo**.
   - En la sección **Tipo de activación**, seleccione un tipo de activación.
     - Para los dispositivos Android, puede seleccionar varios tipos de activación y clasificarlos para satisfacer las necesidades de la empresa.
     - Para los dispositivos Android, si selecciona una tipo de activación Android Enterprise, puede seleccionar la opción **Al activar dispositivos Android Enterprise, active las funciones premium de UEM como BlackBerry Secure Connect Plus.** para activar las funciones BlackBerry Secure Connect Plus y KNOX Platform for Enterprise (para dispositivos que admitan Samsung KNOX).
     - En los dispositivos Android, si selecciona el tipo de activación "Controles de MDM" y no desea que se apliquen las reglas de políticas de KNOX MDM a los dispositivos, desmarque la casilla de verificación **Activar API de Samsung KNOX en activaciones de Controles de MDM**. Esta configuración se aplica únicamente a dispositivos compatibles con KNOX MDM.
     - Para los dispositivos Android, si selecciona uno de los tipos de activación de Samsung KNOX y desea utilizar Google Play para administrar las aplicaciones de trabajo, seleccione **Gestión de aplicaciones de Google Play para dispositivos Samsung Knox Workspace**. Esta opción está disponible únicamente si has configurado una conexión a un dominio de Google. Para obtener más información, consulte el contenido referente a Configuración.
     - Para los dispositivos iOS, si selecciona el tipo de activación "Privacidad del usuario" y desea activar las licencias basadas en SIM, debe seleccionar la opción **Permitir el acceso a la tarjeta SIM y a la información del hardware del dispositivo para activar licencias basadas en SIM**.
     - Para los dispositivos iOS, si selecciona "Controles de MDM" o tipos de activación Privacidad del usuario (con licencias basadas en SIM), puede restringir los dispositivos sin supervisión seleccionando "No permitir activar dispositivos no supervisados".
10. Haga clic en **Agregar**.

Después de terminar: Si fuera necesario, clasifique los perfiles.

Tareas relacionadas

Asignación de un perfil o una política de TI a un grupo de usuarios
Asignar un perfil o una política de TI a una cuenta de usuario
Crear avisos de la empresa

Tipos de activación: dispositivos con BlackBerry 10

Tipo de activación	Descripción
Trabajo y personal - Empresa	Este tipo de activación proporciona el control de los datos del trabajo en los dispositivos, al tiempo que garantiza la máxima privacidad de los datos personales. Al activar un dispositivo, se crea un espacio de trabajo independiente en el dispositivo y el usuario debe crear una contraseña para acceder al espacio de trabajo. Los datos del trabajo se protegen mediante cifrado y la autenticación de contraseña. Todos los datos de trabajo desde cualquiera de las activaciones previas se eliminan. Puede controlar el espacio de trabajo en el dispositivo mediante comandos y políticas de TI, pero no puede controlar ningún aspecto del espacio personal en el dispositivo.
Solo espacio de trabajo	Este tipo de activación proporciona un control completo del dispositivo y no ofrece un espacio independiente para los datos de carácter personal. Al activar un dispositivo, el espacio personal y todos los datos de trabajo de cualquier activación previa se eliminan, se instala un espacio de trabajo y el usuario debe crear una contraseña para acceder al dispositivo. Los datos del trabajo se protegen mediante cifrado y la autenticación de contraseña. Puede controlar el dispositivo a través de comandos y políticas de TI.
Trabajo y personal - Regulado	Este tipo de activación proporciona control tanto sobre los datos personales como sobre los del trabajo. Al activar un dispositivo, se crea un espacio de trabajo independiente en el dispositivo y el usuario debe crear una contraseña para acceder al espacio de trabajo. Los datos del trabajo se protegen mediante cifrado y la autenticación de contraseña. Todos los datos de trabajo desde cualquiera de las activaciones previas se eliminan. Puede controlar tanto el espacio de trabajo como el espacio personal en el dispositivo a través de comandos y políticas de TI.

Tipos de activación: dispositivos iOS

Tipo de activación	Descripción
Controles de MDM	Este tipo de activación proporciona una gestión de dispositivos básica mediante controles de dispositivos puestos a disposición por iOS. No se instala un espacio de trabajo separado en el dispositivo y no hay seguridad adicional para los datos de trabajo. Puede controlar el dispositivo a través de comandos y políticas de TI. Durante la activación, los usuarios deben instalar un perfil de gestión de dispositivos móviles en el dispositivo.
Privacidad del usuario	Puede utilizar el tipo de activación Privacidad del usuario para proporcionar un control básico de los dispositivos a la vez que se garantiza la privacidad de los datos personales de los usuarios. Con este tipo de activación, no se instala ningún contenedor independiente en el dispositivo y no se proporciona seguridad adicional para los datos de trabajo. Los dispositivos activados con Privacidad del usuario se activan en BlackBerry UEM y pueden utilizar servicios como Find my Phone y Root Detection, aunque los administradores no pueden controlar las políticas de los dispositivos. **Nota:** Para licencias basadas en SIM, debe seleccionar "Permitir el acceso a la tarjeta SIM y a la información del hardware del dispositivo para activar licencias basadas en SIM" en el perfil de activación. Los usuarios deben instalar un perfil de MDM que solo pueda tener acceso a la tarjeta SIM y a la información del hardware del dispositivo que se necesita para comprobar si una licencia apropiada de SIM está disponible (por ejemplo, ICCID e IMEI). Los dispositivos Apple TV no admiten este tipo de activación.
Registro del dispositivo solo para BlackBerry 2FA	Este tipo de activación es compatible con la solución de BlackBerry 2FA para dispositivos que BlackBerry UEM no administra. Este tipo de activación no proporciona ningún control o administración de dispositivos, pero permite que los dispositivos utilicen la característica BlackBerry 2FA. Para utilizar este tipo de activación, también debe asignar el perfil BlackBerry 2FA a los usuarios. Cuando se activa un dispositivo, puede ver información limitada de este en la consola de gestión y desactivar el dispositivo mediante un comando. Este tipo de activación solo es compatible con usuarios de Microsoft Active Directory. Los dispositivos Apple TV no admiten este tipo de activación. Para obtener más información, consulte el contenido de BlackBerry 2FA.

Tipos de activación: dispositivos macOS

Tipo de activación	Descripción
Controles de MDM	Este tipo de activación proporciona una gestión de dispositivos básica mediante controles de dispositivos que macOS pone a disposición. Cuando un usuario activa un dispositivo macOS, el dispositivo y el usuario se configuran como entidades independientes en BlackBerry UEM. Se establecen canales de comunicación independientes entre BlackBerry UEM y el dispositivo y entre BlackBerry UEM y la cuenta de usuario, lo que le permite gestionar el dispositivo y el usuario por separado. Algunos perfiles solo se asignan al usuario, por ejemplo, perfiles de correo. Algunos perfiles solo se asignan al dispositivo, por ejemplo, perfiles de proxy. Algunos perfiles le permiten elegir si desea aplicar el perfil al dispositivo o al usuario, por ejemplo, perfiles Wi-Fi. Para obtener más información, consulte Configuraciones de perfil. Puede controlar el dispositivo a través de comandos y políticas de TI. Los usuarios activan los dispositivos macOS mediante BlackBerry UEM Self-Service.

Tipos de activación: dispositivos Android

Para los dispositivos Android, puede seleccionar varios tipos de activación y clasificarlos para asegurarse de que BlackBerry UEM asigne el tipo de activación más adecuada para el dispositivo. Por ejemplo, si clasifica primero "Solo espacio de trabajo (Samsung KNOX)" y segundo "Controles de MDM ", los dispositivos que admiten Samsung KNOX Workspace reciben el primer tipo de activación.

Nota: KNOX MDM permite que el dispositivo utilice las reglas de políticas de TI KNOX MDM en BlackBerry UEM en vez de las reglas básicas disponibles para todos los dispositivos Android. KNOX Workspace crea un espacio de trabajo en el dispositivo que mantiene los datos de trabajo y las aplicaciones de trabajo aparte de los datos personales y las aplicaciones personales.

Los tipos de activación de Android se organizan en las siguientes tablas:

- Dispositivos Android
- Dispositivos Android que utilizan un perfil de trabajo
- Samsung KNOX Workspace

Dispositivos Android

Los siguientes tipos de activación se aplican a todos los dispositivos Android.

Tipo de activación	Descripción
Controles de MDM	Este tipo de activación le permite administrar el dispositivo con comandos y reglas de políticas de TI. Si el dispositivo es compatible con KNOX MDM, este tipo de activación se aplica a las reglas de políticas de TI de KNOX MDM. No se crea un espacio de trabajo separado en el dispositivo y no hay seguridad adicional para los datos de trabajo. Si no desea aplicar las reglas de políticas de KNOX MDM, desmarque la casilla de verificación **Activar Samsung KNOX en dispositivos Samsung que tienen el tipo de activación Controles de MDM asignado**. Esta configuración se aplica únicamente a dispositivos compatibles con KNOX MDM. Durante la activación los usuarios deberán conceder los permisos de administrador a BlackBerry UEM Client. Este tipo de activación quedara en desuso en una versión futura. Para obtener más información, visite http://support.blackberry.com/kb y lea el artículo 47875.
Privacidad del usuario	Puede utilizar el tipo de activación Privacidad del usuario para proporcionar un control básico de los dispositivos a la vez que se garantiza la privacidad de los datos personales de los usuarios. Con este tipo de activación, no se instala ningún contenedor independiente en el dispositivo y no se proporciona seguridad adicional para los datos de trabajo. Los dispositivos activados con Privacidad del usuario se activan en BlackBerry UEM y pueden utilizar servicios como Encuentra mi teléfono y Detección raíz, aunque los administradores no pueden controlar las políticas de los dispositivos.
BlackBerry 2FA	Este tipo de activación es compatible con la solución de BlackBerry 2FA para dispositivos que BlackBerry UEM no administra. Este tipo de activación no proporciona ningún control o administración de dispositivos, pero permite que los dispositivos utilicen la característica BlackBerry 2FA. Para utilizar este tipo de activación, también debe asignar el perfil BlackBerry 2FA a los usuarios. Cuando se activa un dispositivo, puede ver información limitada de este en la consola de gestión y desactivar el dispositivo mediante un comando. Este tipo de activación solo es compatible con usuarios de Microsoft Active Directory. Para obtener más información, consulte el contenido de BlackBerry 2FA.

Dispositivos Android que utilizan un perfil de trabajo

Los siguientes tipos de activación solo se aplican a dispositivos Android que utilizan un perfil de trabajo.

Tipo de activación	Descripción
Trabajo y personal: privacidad de usuario	Este tipo de activación conserva la privacidad de los datos personales, pero le permite administrar los datos de trabajo con comandos y reglas de políticas de TI. Este tipo de activación crea un perfil de trabajo en el dispositivo que separa los datos de trabajo y los datos personales. Los datos personales y los datos de trabajo están protegidos mediante el cifrado y la autenticación de contraseña. Este tipo de activación no es compatible con BlackBerry Secure Connect Plus. Los usuarios no tienen que conceder permisos de administrador a BlackBerry UEM Client.
Trabajo y personal: privacidad de usuario (Premium)	Este tipo de activación conserva la privacidad de los datos personales, pero le permite administrar los datos de trabajo con comandos y reglas de políticas de TI. Este tipo de activación crea un perfil de trabajo en el dispositivo que separa los datos de trabajo y los datos personales. Los datos personales y los datos de trabajo están protegidos mediante el cifrado y la autenticación de contraseña. Los usuarios no tienen que conceder permisos de administrador a BlackBerry UEM Client. Debe utilizar este tipo de activación si desea que se admita BlackBerry Secure Connect Plus con las características del tipo de activación Trabajo y personal: privacidad de usuario.

Tipo de activación	Descripción
Solo espacio de trabajo	Si se asigna este tipo de activación a un usuario, también se le debe asignar la plantilla de correo de activación Solo espacio de trabajo a ese usuario. La asignación de esa plantilla asegura que el usuario reciba el código de activación de Google solicitado durante el proceso de activación. Este tipo de activación le permite administrar todo el dispositivo con comandos y reglas de políticas de TI. Este tipo de activación requiere que el usuario restablezca la configuración predeterminada de fábrica del dispositivo antes de realizar la activación. El proceso de activación instala un perfil de trabajo y no instala ningún perfil personal. El usuario debe crear una contraseña para acceder al dispositivo. Todos los datos del dispositivo estarán protegidos mediante cifrado y un método de autenticación como una contraseña. Este tipo de activación no es compatible con BlackBerry Secure Connect Plus. Durante la activación el dispositivo instala automáticamente BlackBerry UEM Client y le concede permisos de administrador. Los usuarios no pueden revocar los permisos de administrador o desinstalar la aplicación. Si el dispositivo es compatible con KNOX MDM, las siguientes políticas de KNOX MDM también se aplican al dispositivo: • Permitir la autenticación mediante el iris • Permitir la autenticación facial • SSID de Wi-Fi no permitidos • Permitir MMS entrantes • Permitir MMS salientes

Tipo de activación	Descripción
Solo espacio de trabajo (Premium)	Si se asigna este tipo de activación a un usuario, también se le debe asignar la plantilla de correo de activación Solo espacio de trabajo a ese usuario. La asignación de esa plantilla asegura que el usuario reciba el código de activación de Google necesario solicitado durante el proceso de activación. Este tipo de activación le permite administrar todo el dispositivo con comandos y reglas de políticas de TI. Este tipo de activación requiere que el usuario restablezca la configuración predeterminada de fábrica del dispositivo antes de realizar la activación. El proceso de activación instala un perfil de trabajo y no instala ningún perfil personal. El usuario debe crear una contraseña para acceder al dispositivo. Todos los datos del dispositivo estarán protegidos mediante cifrado y un método de autenticación como una contraseña. Este tipo de activación es compatible con el registro de actividad del dispositivo (SMS, MMS y llamadas telefónicas) en archivos de registro de BlackBerry UEM. Durante la activación el dispositivo instala automáticamente BlackBerry UEM Client y le concede permisos de administrador. Los usuarios no pueden revocar los permisos de administrador o desinstalar la aplicación. Debe utilizar este tipo de activación si desea que se admita BlackBerry Secure Connect Plus con las características del tipo de activación Solo espacio de trabajo. Si el dispositivo es compatible con KNOX MDM, las siguientes políticas de KNOX MDM también se aplican al dispositivo: • Permitir la autenticación mediante el iris • Permitir la autenticación facial • SSID de Wi-Fi no permitidos • Permitir MMS entrantes • Permitir MMS salientes • Validar certificados de usuario final instalados

Dispositivos Samsung KNOX Workspace

Los siguientes tipos de activación solo se aplican a dispositivos Samsung compatibles con KNOX Workspace.

Tipo de activación	Descripción
Trabajo y personal: control total (Samsung KNOX)	Este tipo de activación permite administrar todo el dispositivo con comandos y reglas de políticas de TI de KNOX Workspace y MDM de KNOX. Este tipo de activación crea un espacio de trabajo independiente en el dispositivo y el usuario debe crear una contraseña para acceder al espacio de trabajo. Los datos en el espacio de trabajo estarán protegidos mediante cifrado y un método de autenticación como una contraseña, un PIN, un patrón o una huella digital. Este tipo de activación es compatible con el registro de actividad del dispositivo (SMS, MMS y llamadas telefónicas) en archivos de registro de BlackBerry UEM. Durante la activación los usuarios deberán conceder los permisos de administrador a BlackBerry UEM Client.
Trabajo y personal: privacidad de usuario - (Samsung KNOX)	Este tipo de activación conserva la privacidad de los datos personales, pero le permite administrar los datos de trabajo con comandos y reglas de políticas de TI. Este tipo de activación no admite las reglas de políticas de TI de KNOX MDM. Este tipo de activación crea un espacio de trabajo independiente en el dispositivo y el usuario debe crear una contraseña para acceder al espacio de trabajo. Los datos en el espacio de trabajo estarán protegidos mediante cifrado y un método de autenticación como una contraseña, un PIN, un patrón o una huella digital. El usuario también debe crear una contraseña de bloqueo de pantalla para proteger la totalidad del dispositivo y no podrá utilizar el modo de depuración USB. Durante la activación los usuarios deberán conceder los permisos de administrador a BlackBerry UEM Client.
Solo espacio de trabajo - (Samsung KNOX)	Este tipo de activación permite administrar todo el dispositivo con comandos y reglas de políticas de TI de KNOX Workspace y MDM de KNOX. Este tipo de activación elimina el espacio personal e instala un espacio de trabajo. El usuario debe crear una contraseña para acceder al dispositivo. Todos los datos del dispositivo estarán protegidos mediante cifrado y un método de autenticación, como una contraseña, un PIN, un patrón o una huella digital. Este tipo de activación es compatible con el registro de actividad del dispositivo (SMS, MMS y llamadas telefónicas) en archivos de registro de BlackBerry UEM. Durante la activación los usuarios deberán conceder los permisos de administrador a BlackBerry UEM Client.

Tipos de activación: dispositivos Windows

Tipo de activación	Descripción
Controles de MDM	Este tipo de activación proporciona una gestión de dispositivos básica mediante controles de dispositivos puestos a disposición porWindows 10, Windows 10 Mobile, and Windows Phone. No se instala un espacio de trabajo separado en el dispositivo y no hay seguridad adicional para los datos de trabajo. Puede controlar el dispositivo a través de comandos y políticas de TI. Los usuarios de Windows Phone deben instalar BlackBerry UEM Client para activar un dispositivo. Los usuarios de Windows 10 y Windows 10 Mobile activan los dispositivos a través de las aplicaciones de acceso de trabajo de Windows 10.

Activación detallada para usuarios

Si es necesario, puede proporcionar a los usuarios instrucciones detalladas para activar dispositivos.

Activación de dispositivos Android

La información que los usuarios deben introducir y los pasos para activar un dispositivo Android son diferentes dependiendo del tipo de activación que se les ha asignado. Las plantillas de correo de activación contienen la información que los usuarios necesitan. Para obtener más información, consulte Plantillas de correo.

Para las activaciones deQR Code, consulteActivación de un dispositivo mediante QR Code.

Activar un dispositivo Android

Nota: Estos pasos se aplican a un dispositivo asignado al tipo de activación Controles de MDM. Los tipos de activación que instalan o activan un espacio de trabajo en el dispositivo pueden requerir pasos adicionales.

Envíe las siguientes instrucciones de activación para el usuario del dispositivo.

1. Instale BlackBerry UEM Client en el dispositivo. Puede descargar BlackBerry UEM Client desde Google Play.
2. En el dispositivo, toque **UEM Client**.
3. Lea el contrato de licencia. Toque **Acepto**.
4. Escriba su dirección de correo electrónico de trabajo. Toque **Siguiente**.
5. Si es necesario, escriba la dirección del servidor. Toque **Siguiente**. Puede encontrar la dirección del servidor en el mensaje de correo de activación que ha recibido o en BlackBerry UEM Self-Service.
6. Escriba una contraseña de activación. Toque **Activar mi dispositivo**.
7. Toque **Siguiente**.
8. Toque **Activar**.

Después de terminar: Para verificar que el proceso de activación se ha completado correctamente, realice una de las siguientes acciones:

- En el dispositivo, abra BlackBerry UEM Client. Toque **Acerca de**. En la sección **Dispositivo activado**, compruebe que la información del dispositivo y la marca de tiempo de activación están presentes.
- En BlackBerry UEM Self-Service, compruebe que el dispositivo aparezca como un dispositivo activado. El estado puede tardar hasta dos minutos en actualizarse una vez que haya activado el dispositivo.

Activar un dispositivo Android que tenga un perfil de trabajo

Estos pasos se aplican a dispositivos a los que se han asignado uno de los siguientes tipos de activación:

- Trabajo y personal: privacidad de usuario
- Trabajo y personal: privacidad de usuario (Premium)

Envíe las instrucciones de activación siguientes al usuario del dispositivo.

Antes de empezar:

- Necesitará la información siguiente:
  - Contraseña de activación de BlackBerry UEM
  - Su correo de trabajo y contraseña
- Puede que necesite la siguiente información:
  - Dirección del servidor de BlackBerry UEM
  - Contraseña de la cuenta de Google

1. Instale BlackBerry UEM Client en el dispositivo. Puede descargar BlackBerry UEM Client desde Google Play.
2. En el dispositivo, toque **UEM Client**.
3. Lea el contrato de licencia. Toque **Acepto**.
4. Escriba su dirección de correo electrónico de trabajo. Toque **Siguiente**.
5. Si es necesario, escriba la dirección del servidor. Toque **Siguiente**. Puede encontrar la dirección del servidor en el mensaje de correo de activación que ha recibido o en BlackBerry UEM Self-Service.
6. Escriba una contraseña de activación. Toque **Activar mi dispositivo**.
7. Espere mientras la configuración y los perfiles se cargan en el dispositivo.
8. Toque **Configurar**.
9. Toque **Aceptar** y espere mientras el perfil de trabajo se configura.
10. Si es necesario, escriba la contraseña de Google. Toque **Siguiente**.
11. Si se le solicita, puede configurar una contraseña del dispositivo y seleccionar las opciones de notificación.
12. Si se le solicita, toque **Aceptar** para permitir la conexión con BlackBerry Secure Connect Plus y espere mientras la conexión esté activada.

Activación de un dispositivo con perfiles de trabajo de Android con un único espacio de trabajo

Estos pasos se aplican a dispositivos a los que se han asignado uno de los siguientes tipos de activación:

- Solo espacio de trabajo
- Solo espacio de trabajo (Premium)

Envíe las instrucciones de activación siguientes al usuario del dispositivo.

Antes de empezar: Asegúrese de que dispone de la siguiente información que envió el administrador en uno o más mensajes de correo electrónico:

- Contraseña de activación de BlackBerry UEM
- Código de activación del perfil de trabajo de Android
- Su correo de trabajo y contraseña
- La dirección del servidor de BlackBerry UEM (puede que no la necesite)

1. Si no ve la pantalla de bienvenida de configuración del dispositivo, restablezca el dispositivo con la configuración predeterminada de fábrica.

2. Durante la configuración del dispositivo, en la pantalla **Agregar su cuenta**, toque **Menú > Configurar dispositivo de trabajo**.
3. Si se solicita, cifre el dispositivo.
4. En el dispositivo, toque **UEM Client**.
5. Lea el contrato de licencia. Toque **Acepto**.
6. Escriba su dirección de correo electrónico de trabajo. Toque **Siguiente**.
7. Si es necesario, escriba la dirección del servidor. Toque **Siguiente**. Puede encontrar la dirección del servidor en el mensaje de correo de activación que ha recibido o en BlackBerry UEM Self-Service.
8. Escriba una contraseña de activación. Toque **Activar mi dispositivo**.
9. Espere mientras la configuración y los perfiles se cargan en el dispositivo.
10. Toque **Configurar**.
11. Toque **Aceptar** y espere mientras el perfil de trabajo se configura.
12. Escriba la contraseña de Google.
13. Toque **Siguiente**.
14. En la pantalla **Desbloquear selección**, toque **Contraseña**.
15. Asegúrese de que **Requerir una contraseña para iniciar el dispositivo** está seleccionado. Toque **Continuar**.
16. Escriba una contraseña del dispositivo y vuelva a escribirla para confirmarla. Toque **Aceptar**.
17. Seleccione una de las opciones para especificar cómo desea que se muestren las notificaciones. Toque **Hecho**.
18. Si se solicita, toque **Aceptar** para permitir la conexión con BlackBerry Secure Connect Plus y espere mientras la conexión esté activada.
19. Desde la pantalla de inicio, abra la lista de aplicaciones. Toque la aplicación BlackBerry Hub para completar la configuración.
    a) Toque **Siguiente** para otorgar permisos a los servicios BlackBerry en su dispositivo y si se solicita, toque **Permitir** para cada una de las siguientes pantallas.
    b) Toque la flecha para continuar.
    c) Toque **Conceder permisos** para conceder permisos a BlackBerry Hub en el dispositivo. Si se solicita, seleccione **Permitir** para cada una de las siguientes pantallas.
    d) Toque su dirección de correo.
    e) Escriba la contraseña de la dirección de correo de trabajo. Toque **Siguiente**.
    f) Toque **Aceptar**.
    g) En la pantalla **Administración de seguridad remota**, toque **Aceptar**.
    h) En la pantalla **Configuración de cuentas**, toque **Siguiente**.
    i) En la pantalla **Actualización de seguridad**, toque **Aceptar**.
    j) Toque **Activar** para activar el administrador de dispositivos.
    k) Toque **Hecho**.
20. Navegue por BlackBerry Hub y espere a que sus mensajes de correo se sincronicen.

Activación de un dispositivo Android con un único espacio de trabajo y sin dominio de Google

Estos pasos se aplican a dispositivos a los que se han asignado uno de los siguientes tipos de activación:

- Solo espacio de trabajo
- Solo espacio de trabajo (Premium)

Envíe las instrucciones de activación siguientes al usuario del dispositivo.

Antes de empezar: Asegúrese de que dispone de la siguiente información que envió el administrador en uno o más mensajes de correo electrónico:

- Nombre de usuario de activación
- Contraseña de activación de BlackBerry UEM

1. Si no ve la pantalla de bienvenida de configuración del dispositivo, restablezca el dispositivo con la configuración predeterminada de fábrica.
2. Durante la configuración del dispositivo, en la pantalla **Agregar su cuenta**, escriba afw#blackberry.
3. Espere mientras el dispositivo actualiza las aplicaciones del sistema y descarga BlackBerry UEM Client.
4. Lea el contrato de licencia. Toque **Acepto**.
5. Escriba su dirección de correo electrónico de trabajo. Toque **Siguiente**.
6. Si es necesario, escriba la dirección del servidor. Toque **Siguiente**. Puede encontrar la dirección del servidor en el mensaje de correo de activación que ha recibido o en BlackBerry UEM Self-Service.
7. Escriba una contraseña de activación. Toque **Activar mi dispositivo**.
8. Espere mientras la configuración y los perfiles se cargan en el dispositivo.
9. Toque **Configurar**.
10. Toque **Aceptar** y espere mientras el perfil de trabajo se configura.
11. Escriba la contraseña de Google.
12. Toque **Siguiente**.
13. En la pantalla **Desbloquear selección**, toque **Contraseña**.
14. Asegúrese de que **Requerir una contraseña para iniciar el dispositivo** está seleccionado. Toque **Continuar**.
15. Escriba una contraseña del dispositivo y vuelva a escribirla para confirmarla. Toque **Aceptar**.
16. Seleccione una de las opciones para especificar cómo desea que se muestren las notificaciones. Toque **Hecho**.
17. Si se le solicita, toque **Aceptar** para permitir la conexión con BlackBerry Secure Connect Plus y espere mientras la conexión esté activada.
18. Desde la pantalla de inicio, abra la lista de aplicaciones. Toque la aplicación BlackBerry Hub para completar la configuración.
    a) Toque **Siguiente** para otorgar permisos a los servicios BlackBerry en su dispositivo y si se solicita, toque **Permitir** para cada una de las siguientes pantallas.
    b) Toque la flecha para continuar.
    c) Toque **Conceder permisos** para otorgar permisos a BlackBerry Hub en su dispositivo. Si se solicita, toque **Permitir** para cada una de las siguientes pantallas.
    d) Toque su dirección de correo.
    e) Escriba la contraseña de la dirección de correo de trabajo. Toque **Siguiente**.
    f) Toque **Aceptar**.
    g) En la pantalla **Administración de seguridad remota**, toque **Aceptar**.
    h) En la pantalla **Configuración de cuentas**, toque **Siguiente**.
    i) En la pantalla **Actualización de seguridad**, toque **Aceptar**.
    j) Toque **Activar** para activar el administrador de dispositivos.
    k) Toque **Hecho**.
19. Navegue por BlackBerry Hub y espere a que sus mensajes de correo se sincronicen.

Activar un dispositivo iOS

Para las activaciones deQR Code, consulteActivación de un dispositivo mediante QR Code.

Para activar los dispositivos mediante una contraseña de activación, envíe las siguientes instrucciones al usuario del dispositivo.

1. Instale la aplicación BlackBerry UEM Client en el dispositivo. Puede descargar la aplicación BlackBerry UEM Client desde App Store.
2. En el dispositivo, toque **UEM Client**.
3. Lea el contrato de licencia y toque **Acepto**.
4. Escriba su dirección de correo de trabajo y toque **Ir**.
5. Si es necesario, escriba la dirección del servidor y toque **Ir**. Puede encontrar la dirección del servidor en el mensaje de correo de activación que ha recibido o en BlackBerry UEM Self-Service.
6. Escriba la contraseña de activación y toque **Activar mi dispositivo**.
7. Toque **Aceptar** para instalar el certificado necesario.
8. Siga las instrucciones que aparecen en pantalla para completar la instalación.
9. Si se le solicita introducir la contraseña de su cuenta de correo electrónico o el código secreto de su dispositivo, siga las instrucciones que aparecen en la pantalla.

Después de terminar: Para verificar que el proceso de activación se ha completado correctamente, realice una de las siguientes acciones:

- En el dispositivo, abra la aplicación BlackBerry UEM Client y toque **Acerca de**. En las secciones Dispositivo activado y Estado de conformidad, verifique que aparezcan la información de dispositivo y la marca de tiempo de activación.
- En BlackBerry UEM Self-Service, verifique que el dispositivo aparezca como un dispositivo activado. El estado puede tardar hasta dos minutos en actualizarse una vez que haya activado el dispositivo.

Activar un dispositivo BlackBerry 10

Envíe las instrucciones de activación siguientes al usuario del dispositivo.

1. En el dispositivo, diríjase a **Configuración**.
2. Toque **Cuentas**.
3. Si tiene cuentas en este dispositivo, toque **Agregar cuenta**. De lo contrario, continúe con el paso 4.
4. Toque **Correo, calendario y contactos**.
5. Escriba su dirección de correo de trabajo y toque **Siguiente**.
6. En el campo **Contraseña**, escriba la contraseña de activación que recibió. Toque **Siguiente**.
7. Si recibe una advertencia de que el dispositivo no puede consultar la información de conexión, realice los siguientes pasos:
   a) Toque **Avanzado**.
   b) Toque **Cuenta de trabajo**.
   c) En el campo **Dirección del servidor**, escriba la dirección del servidor. Puede encontrar la dirección del servidor en el mensaje de correo de activación que ha recibido o en BlackBerry UEM Self-Service.
   d) Toque **Hecho**.
8. Siga las instrucciones que aparecen en pantalla para completar el proceso de activación.

Después de terminar: Para comprobar que el proceso de activación se ha completado correctamente, realice una de las siguientes acciones:

- En el dispositivo, diríjase al BlackBerry Hub y confirme que aparece la dirección de correo. Vaya al calendario y confirme que aparecen las citas.
- En BlackBerry UEM Self-Service, compruebe que el dispositivo aparezca como un dispositivo activado. El estado puede tardar hasta dos minutos en actualizarse una vez que haya activado el dispositivo.

Activar un dispositivo Windows Phone

Envíe las instrucciones de activación siguientes al usuario del dispositivo.

1. Instale BlackBerry UEM Client en el dispositivo. Puede descargar BlackBerry UEM Client desde .
2. En el dispositivo, vaya a la lista de aplicaciones y toque **UEM Client**.
3. Lea el contrato de licencia y toque **Acepto**.
4. Escriba su dirección de correo de trabajo y toque **siguiente**.
5. Si es necesario, escriba la dirección del servidor y toque **siguiente**. Puede encontrar la dirección del servidor en el mensaje de correo de activación que ha recibido o en BlackBerry UEM Self-Service.
6. Escriba la contraseña de activación que recibió en el mensaje de correo de activación o que estableció en BlackBerry UEM Self-Service y toque **Activar mi dispositivo**.
7. Toque **copiar y continuar** para copiar la dirección del servidor y vaya a la aplicación del espacio de trabajo Windows Phone.
8. Toque **agregar cuenta**.
9. Escriba su dirección de correo y toque **iniciar sesión**.
10. Con el cursor en el campo Servidor, toque el icono **Pegar**.
11. Toque **iniciar sesión**.
12. Si recibe una advertencia acerca del certificado, toque **Continuar**.
13. Deje los campos Nombre de usuario y Dominio en blanco. En el campo Contraseña, escriba la contraseña de activación que recibió en el mensaje de correo de activación o que estableció en BlackBerry UEM Self-Service. Toque **iniciar sesión**.
14. Toque **hecho**.
15. Pulse el botón **Atrás** del Windows Phone para volver a BlackBerry UEM Client.
16. La activación se completa automáticamente.

Después de terminar: Para comprobar que el proceso de activación se ha completado correctamente, realice una de las siguientes acciones:

- En el dispositivo, abra BlackBerry UEM Client, toque el icono de **Menú** en la parte inferior derecha (tres puntos horizontales) y toque **Acerca de**. En la sección Dispositivo activado, compruebe que la información de dispositivo y la marca de tiempo de activación están presentes.
- En BlackBerry UEM Self-Service, compruebe que el dispositivo aparezca como un dispositivo activado. El estado puede tardar hasta dos minutos en actualizarse una vez que haya activado el dispositivo.

Activar un dispositivo Windows 10 Mobile

Envíe las instrucciones de activación siguientes al usuario del dispositivo.

1. En el navegador de su dispositivo, escriba o pegue la dirección del servidor de certificados. Puede encontrar la dirección del servidor de certificados en el mensaje de correo de activación que ha recibido. Si no ha recibido un vínculo al certificado, póngase en contacto con su administrador para obtener asistencia.
2. Toque el certificado.
3. Toque **Instalar**.
4. Toque **Aceptar**.
5. Toque el botón **Windows** para volver al menú Inicio.
6. Deslice el dedo hacia la izquierda para abrir el menú de aplicaciones.
7. Lleve a cabo una de las tareas siguientes:

Versión del SO del dispositivo	Pasos
Windows 10 versión 1607 o posterior	**a.** Toque **Configuración > Cuentas > Acceso de trabajo o escuela**. **b.** Toque **Inscribir solo en gestión de dispositivos**.

Versión del SO del dispositivo	Pasos
Windows 10 versión anterior a 1607	**a.** Toque **Configuración > Cuentas > Acceso de trabajo**. **b.** Toque **Conectarse**.

8. En el campo **Dirección de correo**, escriba su dirección de correo de trabajo y toque **Intro**.
9. Si se solicita, en el campo **Servidor**, escriba el nombre del servidor y toque **Continuar**. Puede encontrar el nombre del servidor en el correo de activación que ha recibido de su administrador o en BlackBerry UEM Self-Service cuando establece la contraseña de activación.
10. En el campo **Contraseña de activación**, escriba la contraseña de activación y toque **Continuar**. Puede encontrar la contraseña de activación en el correo que ha recibido de su administrador o puede establecer su propia contraseña de activación en BlackBerry UEM Self-Service.
11. Toque **Finalizado**.
12. El proceso de activación se ha completado.

Después de terminar:

- Para verificar que el proceso de activación se ha completado correctamente, puede realizar una de las siguientes acciones:
  - En el dispositivo, haga clic en Configuración > Cuentas > Acceso de trabajo o escuela (o Acceso de trabajo) para confirmar que el dispositivo está conectado a BlackBerry UEM. Haga clic en el icono del maletín > Información para comprobar la información del estado de la sincronización.
  - En BlackBerry UEM Self-Service, compruebe que el dispositivo aparezca como un dispositivo activado. El estado puede tardar hasta dos minutos en actualizarse una vez que haya activado el dispositivo.
- Si se solicita por parte del administrador, agregue su cuenta de trabajo a Cuentas utilizadas por otras aplicaciones para que pueda acceder a las aplicaciones en línea necesarias.
  - Para Windows 10 versión 1607 o posterior, haga clic en Configuración > Cuentas > Acceso de trabajo y escuela > Conectar. Escriba su dirección de correo de trabajo y contraseña.
  - Para Windows 10 versión anterior a 1607, haga clic en Configuración > Cuentas > Sus cuentas y correo electrónico. En Cuentas utilizadas por otras aplicaciones, haga clic en Agregar una cuenta de trabajo o escuela y escriba la dirección de correo de trabajo y la contraseña.

Activar un dispositivo macOS

Envíe las instrucciones de activación siguientes al usuario del dispositivo.

Antes de empezar: Necesitará la siguiente información de inicio de sesión de BlackBerry UEM Self-Service:

- Dirección web de BlackBerry UEM Self-Service
- Nombre de usuario y contraseña
- Nombre de dominio

1. Inicie sesión en BlackBerry UEM Self-Service con el dispositivo que desea activar y la información de inicio de sesión que ha recibido de su administrador.
2. Si ya se muestran dispositivos, haga clic en **Activar un dispositivo**.
3. En el menú desplegable Dispositivo, haga clic en **macOS**.
4. Vea el tutorial de activación.
5. Haga clic en **Enviar**.
6. Siga las instrucciones para instalar los perfiles requeridos y completar la activación del dispositivo. Cuando termine la activación, podrá ver su dispositivo en BlackBerry UEM Self-Service.

Activar un dispositivo Apple TV

Envíe las instrucciones de activación siguientes al usuario del dispositivo.

Antes de empezar:

- Necesita la dirección web y las credenciales de inicio de sesión para BlackBerry UEM Self-Service.
- Necesita un ordenador macOS con Apple Configurator 2 instalado.
- Necesita un cable USB C o micro USB (en función de la versión de Apple TV).
- Compruebe que el dispositivo Apple TV está en modo supervisado.
- Desconecte el cable HDMI y el cable de alimentación del dispositivo Apple TV.

1. Conecte el dispositivo Apple TV al ordenador macOS mediante un cable USB C o micro USB.
2. Para las versiones de tercera y cuarta generación de Apple TV, conecte el cable de alimentación.
3. En el equipo macOS, inicie sesión en BlackBerry UEM Self-Service.
4. Dependiendo de si está activado su primer dispositivo o de si ya ha activado alguno antes, haga clic en o bien, haga clic en > **Activar un dispositivo**.
5. En el menú desplegable Dispositivo, haga clic en **Apple TV**.
6. Haga clic en **Submit**.
7. Haga clic en **Descargar perfil**.
8. Haga clic en **Cerrar**.
9. Abra Apple Configurator 2.
10. Seleccione Apple TV y haga clic en **Agregar > Perfiles**.
11. Seleccione el archivo de configuración que ha descargado en el paso 7 y haga clic en **Agregar**.
12. Cuando termine la activación, podrá ver su dispositivo en BlackBerry UEM Self-Service.

Active una tableta o un equipo Windows 10

Nota: Si desea gestionar dispositivos con Windows 10 mediante MDM, Microsoft System Center Configuration Manager no puede gestionar dichos dispositivos.

Envíe las instrucciones de activación siguientes al usuario del dispositivo.

1. En el navegador de su dispositivo, escriba o pegue la dirección del servidor de certificados. Puede encontrar la dirección del servidor de certificados en el mensaje de correo de activación que ha recibido. Si no ha recibido un vínculo al certificado, póngase en contacto con su administrador para obtener asistencia.
2. Haga clic en **Guardar**.
3. En la notificación de descarga del certificado, toque **Abrir**.
4. Haga clic en **Abrir**.
5. Haga clic en **Instalar certificado**.
6. Seleccione la opción **Usuario actual**. Haga clic en **Siguiente**.
7. Seleccione la opción **Colocar todos los certificados en el siguiente almacén**. Haga clic en **Examinar**.
8. Seleccione **Autoridades de certificación raíz de confianza**. Haga clic en **Aceptar**.
9. Haga clic en **Siguiente**.
10. Haga clic en **Finish (Finalizar)**.
11. Haga clic en **Aceptar**.
12. Haga clic en **Aceptar**.
13. Haga clic en el botón **Inicio**.
14. Lleve a cabo una de las tareas siguientes:

Versión del SO del dispositivo	Pasos
Windows 10 versión 1607 o posterior	**a.** Toque **Configuración > Cuentas > Acceso de trabajo o escuela**. **b.** Toque **Inscribir solo en gestión de dispositivos**.
Windows 10 versión anterior a 1607	**a.** Toque **Configuración > Cuentas > Acceso de trabajo**. **b.** Toque **Conectarse**.

15. En el campo **Dirección de correo**, escriba su dirección de correo. Toque **Continuar**.
16. Si se solicita, en el campo **Servidor**, escriba el nombre del servidor y toque **Continuar**. Puede encontrar el nombre del servidor en el correo de activación que ha recibido de su administrador o en BlackBerry UEM Self-Service cuando establece la contraseña de activación.
17. En el campo **Contraseña de activación**, escriba la contraseña de activación y toque **Continuar**. Puede encontrar la contraseña de activación en el correo de activación que ha recibido de su administrador o puede establecer su propia contraseña de activación en BlackBerry UEM Self-Service.
18. Toque **Hecho**.
19. El proceso de activación se ha completado.

Después de terminar:

- Para verificar que el proceso de activación se ha completado correctamente, puede realizar una de las siguientes acciones:
  - En el dispositivo, haga clic en Configuración > Cuentas > Acceso de trabajo o escuela (o Acceso de trabajo) para confirmar que el dispositivo está conectado a BlackBerry UEM. Haga clic en el icono del maletín > Información para comprobar la información del estado de la sincronización.
  - En BlackBerry UEM Self-Service, compruebe que el dispositivo aparezca como un dispositivo activado. El estado puede tardar hasta dos minutos en actualizarse una vez que haya activado el dispositivo.
- Si se solicita por parte del administrador, agregue su cuenta de trabajo a Cuentas utilizadas por otras aplicaciones para que pueda acceder a las aplicaciones en línea necesarias.
  - Para Windows 10 versión 1607 o posterior, haga clic en Configuración > Cuentas > Acceso de trabajo y escuela > Conectar. Escriba su dirección de correo de trabajo y contraseña.
  - Para Windows 10 versión anterior a 1607, haga clic en Configuración > Cuentas > Sus cuentas y correo electrónico. En Cuentas utilizadas por otras aplicaciones, haga clic en Agregar una cuenta de trabajo o escuela y escriba la dirección de correo de trabajo y la contraseña.

Activación de un dispositivo mediante QR Code

La activación QR Code es compatible con los dispositivos iOS y Android.

Para activar los dispositivos mediante QR Code, envíe las siguientes instrucciones al usuario del dispositivo.

Antes de empezar: Necesita contar con QR Code. Se puede encontrar en el correo de activación que ha recibido de su administrador, o bien se puede generar en BlackBerry UEM Self-Service.

1. Instale la aplicación BlackBerry UEM Client en el dispositivo. Para los dispositivos iOS, descargue la aplicación de App Store. Para los dispositivos Android, descargue la aplicación de Google Play.
2. En el dispositivo, toque **UEM Client**.
3. Lea el contrato de licencia y toque **Acepto**.
4. Busque la QR Code que ha recibido en el correo de activación o que ha generado en BlackBerry UEM Self-Service.
5. Si se le solicita introducir la contraseña de su cuenta de correo electrónico o el código secreto de su dispositivo, siga las instrucciones que aparecen en la pantalla.

Después de terminar: Para verificar que el proceso de activación se ha completado correctamente, puede realizar una de las siguientes acciones:

- En el dispositivo, abra la aplicación BlackBerry UEM Client y toque **Acerca de**. En las secciones Dispositivo activado y Estado de conformidad, compruebe que aparezcan la información de dispositivo y la marca de tiempo de activación.
- En BlackBerry UEM Self-Service, compruebe que el dispositivo aparezca como un dispositivo activado. El estado puede tardar hasta dos minutos en actualizarse una vez que haya activado el dispositivo.

Activación de un dispositivo BlackBerry OS

Envíe las instrucciones de activación siguientes al usuario del dispositivo.

1. En el dispositivo, vaya a **Configuración**.
2. Haga clic en **Cuentas de correo**.
3. Haga clic en **Cuenta de empresa**.
4. En el campo **Correo**, escriba su dirección de correo de trabajo.
5. En el campo **Contraseña**, escriba la contraseña de activación que recibió.
6. Haga clic en **Activar**.
7. Haga clic en **Aceptar.**

Después de terminar: Para comprobar que el proceso de activación se ha completado correctamente, realice una de las siguientes acciones:

- En el dispositivo, vaya a la aplicación Configuración y haga clic en **Cuentas de correo**. Confirme que aparece la dirección de correo.
- En BlackBerry Web Desktop Manager, compruebe que el dispositivo aparezca como un dispositivo activado. El estado puede tardar hasta dos minutos en actualizarse una vez que haya activado el dispositivo.

Active varios dispositivos mediante KNOX Mobile Enrollment

Samsung KNOX Mobile Enrollment le permite activar un gran número de dispositivos en BlackBerry UEM a la vez. Para obtener más información, visite https://www.samsungknox.com/en/products/knox-mobile-enrollment.

Antes de empezar: Debe comprar sus dispositivos a través de una de las siguientes opciones:

- Un distribuidor homologado
- Un distribuidor dispuesto a compartir el IMEI del dispositivo directamente con Samsung

1. En la barra de menús, haga clic en **Configuración > Integración externa**.
2. Haga clic en **KNOX Mobile Enrollment**.
3. Siga los pasos que aparecen en pantalla.

Después de terminar: Después de completar la activación, haga clic en **Descargar** para descargar el archivo configuration.json. En el archivo, compare la entrada en la sección CFPrint con la entrada que ha añadió al configurar KNOX Mobile Enrollment. Si las entradas son diferentes, copie el texto completo del archivo .json en el campo Custom JSON Data de la página KNOX Mobile Enrollment.

Activar varios dispositivos mediante inscripción desatendida para dispositivos Android

La inscripción desatendida le permite implementar un gran número de dispositivos Android a la vez.

Su empresa compra estos dispositivos a un distribuidor de empresa autorizado, que configura una cuenta de inscripción desatendida y agrega los dispositivos a la cuenta para aprovisionarlos para la gestión de dispositivos. Cuando los usuarios configuran estos dispositivos por primera vez, los dispositivos descargan automáticamente BlackBerry UEM Client e inician el proceso de activación con BlackBerry UEM. El usuario debe completar el proceso de activación para utilizar el dispositivo.

Para obtener más información sobre la inscripción desatendida y cómo configurarla, consulte https://www.android.com/intl/en_ca/enterprise/management/zero-touch/ y https://support.google.com/work/android/answer/7514005.

Para utilizar la inscripción desatendida en BlackBerry UEM, los dispositivos deben ejecutar Android 8.0 o posterior y estar activados para inscripción desatendida.

1. Compre dispositivos compatibles a un distribuidor de empresa autorizado. El distribuidor configura una cuenta de inscripción desatendida para su empresa.
2. En la plataforma desatendida, el distribuidor agrega los dispositivos que ha comprado.
3. En la consola de gestión de BlackBerry UEM, en la barra de menú, haga clic en **Configuración > Integración externa**.
4. Haga clic en **Empresa con Android**.
5. En la parte inferior de la pantalla, haga clic en **Más información**.
6. Copie la cadena generada por esta instancia de BlackBerry UEM para utilizarla en la configuración de dispositivos en el portal de inscripción desatendida.

   Puede dejar en blanco el campo de nombre de usuario o editarlo para incluir un nombre de usuario de modo que solo se pueda utilizar dicho nombre para iniciar sesión en el dispositivo que utiliza la configuración.
7. En la plataforma desatendida, cree configuraciones y asígnelas a los dispositivos que ha comprado.
8. En BlackBerry UEM, compruebe que los perfiles y las políticas de TI adecuados se han asignado a los usuarios. Para utilizar la inscripción desatendida, debe asignar un perfil de activación con el tipo de activación "Solo espacio de trabajo" o "Solo espacio de trabajo (Premium)" activado.
9. Distribuya los dispositivos a los usuarios.

Activación de los dispositivos iOS que están inscritos en DEP

Puede inscribir los dispositivos iOS en el programa de inscripción de dispositivos de Apple y asignar configuraciones de inscripción para dispositivos mediante la consola de gestión de BlackBerry UEM. Las configuraciones de inscripción incluyen reglas adicionales, tales como "Activar modo supervisado", que se asignan a los dispositivos durante la inscripción de MDM.

Puede utilizar una cuenta de Apple Business Manager parta sincronizar BlackBerry UEM con DEP. Apple Business Manager es un portal basado en web en el que puede inscribir y gestionar dispositivos iOS en DEP, así como gestionar cuentas VPP de Apple. Si su empresa utiliza DEP o VPP, puede actualizar a Apple Business Manager.

Cuando los dispositivos están activados, BlackBerry UEM envía las políticas y los perfiles de TI que se asignan a los usuarios.

Nota: Para que funcionen determinadas funciones, debe asignar la aplicación BlackBerry UEM Client a los usuarios. Los usuarios deben iniciar BlackBerry UEM Client después de activar el dispositivo. Para obtener más información sobre cuándo debe asignar la aplicación BlackBerry UEM Client a los usuarios, visite support.blackberry.com/kb/ para leer el artículo KB39313.

Pasos para activar los dispositivos que están inscritos en DEP

Al activar los dispositivos iOS que están inscritos en el programa de inscripción de dispositivos de Apple, deberá realizar las siguientes acciones:

Paso	Acción
1	Registro de dispositivos iOS en DEP y su asignación a un servidor BlackBerry UEM.
2	Si no seleccionó "Asignar automáticamente los nuevos dispositivos a esta configuración" cuando creó la configuración de inscripción, o bien si desea asignar una configuración diferente, asigne una configuración de inscripción.
3	También puede agregar la aplicación de BlackBerry UEM Client a la lista de aplicaciones y asignarla a las cuentas o grupos de usuarios. Consulte Adición de una aplicación de iOS a la lista de aplicaciones.
4	Si no desea utilizar el perfil de activación predeterminado, consulte Creación de un perfil de activación y su asignación a una cuenta de usuario o a un grupo al que pertenezca el usuario.
5	Establezca una contraseña de activación para el usuario y envíe un correo electrónico de activación a los usuarios mediante la plantilla de correo de Apple DEP. Cuando establezca la contraseña de activación, debe seleccionar la opción "Activación del dispositivo predeterminada". Los usuarios del directorio de la empresa pueden utilizar su nombre de usuario y contraseña del directorio de la empresa para que no tenga que crear una contraseña de activación. Los usuarios deben introducir su nombre de usuario en el formato dominio \nombre de usuario.
6	Distribuya los dispositivos a los usuarios y solicite que completen la instalación. Tras finalizar la configuración, los usuarios deben instalar y abrir la aplicación BlackBerry UEM Client.

Registro de dispositivos iOS en DEP y su asignación a un servidor BlackBerry UEM

Para registrar los dispositivos, debe introducir los números de serie del dispositivo en el portal de DEP o Apple Business Manager y asignar los dispositivos a un servidor BlackBerry UEM. Puede introducir los números de serie de las siguientes formas:

- Escribir cada número
- Seleccionar el número de orden que Apple asignó a los dispositivos cuando los adquirió
- Cargar un archivo .csv que contenga los números de serie

Antes de empezar: Configure BlackBerry UEM para utilizar DEP. Para obtener más información, consulte el contenido de Configuración.

1. En un navegador, escriba **business.apple.com** o **deploy.apple.com**.
2. Inicie sesión en la cuenta de DEP o Apple Business Manager.
3. En la sección **Programa de inscripción de dispositivos**, haga clic en **Gestionar dispositivos**.
4. Siga los pasos para introducir los números de serie de los dispositivos.
5. Asigne los números de serie al servidor BlackBerry UEM.

Después de terminar: Asignación de una configuración de inscripción a dispositivos iOS.

Asignación de una configuración de inscripción a dispositivos iOS

Si ha creado una configuración de inscripción y ha seleccionado "Asignar automáticamente todos los nuevos dispositivos a esta configuración", BlackBerry UEM asigna automáticamente la configuración cuando los dispositivos DEP se sincronicen con BlackBerry UEM. De lo contrario, debe asignar una configuración de inscripción a los dispositivos. BlackBerry UEM se sincroniza con DEP a diario y siempre que se visualiza la página de dispositivos DEP de Apple.

Si el estado de activación de un dispositivo aún está pendiente, puede eliminar la configuración de inscripción existente y asignar una nueva.

Antes de empezar: Registro de dispositivos iOS en DEP y su asignación a un servidor BlackBerry UEM.

1. En la barra de menú, haga clic en **Usuarios > Dispositivos de Apple DEP**.
2. Seleccione las casillas de verificación situadas junto a los dispositivos a los que desea asignar una configuración de inscripción. Debe seleccionar dispositivos que estén registrados a la misma cuenta de DEP.
3. Haga clic en .
4. En la lista desplegable **Configuración de inscripción**, seleccione la configuración de inscripción que desea asignar.
5. Haga clic en **Asignar**.

Después de terminar: Distribuya los dispositivos iOS a los usuarios. Como parte de la configuración del dispositivo, los dispositivos se activan con BlackBerry UEM. Se solicita a los usuarios un nombre de usuario y una contraseña. Los usuarios del directorio de la empresa pueden utilizar su nombre de usuario del directorio de la empresa (en el formato dominio\nombre de usuario) y la contraseña. Los usuarios locales necesitan utilizar una contraseña de activación. Consulte Establezca una contraseña de activación para el usuario.

Adición de una configuración de inscripción

Una configuración de inscripción le permite definir cómo se configuran los dispositivos que están inscritos en DEP cuando se activan en BlackBerry UEM. Puede crear tantas configuraciones de inscripción como necesite la empresa.

1. En la barra de menú, haga clic en **Configuración**.
2. En el panel izquierdo, haga clic en **Integración externa > Programa de inscripción de dispositivos de Apple**.
3. Haga clic en el nombre de una cuenta de DEP.
4. En la sección **Configuraciones de inscripción de DEP**, haga clic en +.
5. Escriba un nombre para la configuración.
6. Complete una de las tareas siguientes:
   - Si desea que BlackBerry UEM asigne automáticamente la configuración de inscripción cuando los dispositivos DEP se sincronicen con BlackBerry UEM, seleccione la casilla para marcar "Asignar automáticamente todos los nuevos dispositivos a esta configuración". BlackBerry UEM se sincroniza con Apple DEP a diario y siempre que se visualiza la página de dispositivos DEP de Apple.

     Nota: Si previamente se creó una configuración de inscripción con esta configuración y se aplicó a los dispositivos, BlackBerry UEM no asigna la nueva configuración de inscripción.

     Nota: Solo puede seleccionar una configuración de inscripción para que se asigne automáticamente a nuevos dispositivos de DEP. Si ha creado previamente una configuración de inscripción con esta configuración, la configuración se elimina de la configuración anterior y se agrega a la nueva.
   - Si desea asignar manualmente la configuración de inscripción a dispositivos específicos, no seleccione la casilla para marcar "Asignar automáticamente todos los nuevos dispositivos a esta configuración".
7. Opcionalmente, escriba el nombre de un departamento y un número de teléfono de soporte para que se muestren en los dispositivos durante la instalación.

8. En la sección **Configuración del dispositivo**, seleccione entre las siguientes opciones:
   - Permitir emparejamiento: si esta opción está seleccionada, los usuarios pueden emparejar el dispositivo con un ordenador
   - Activar modo supervisado: si esta opción está seleccionada, los dispositivos se activan en el modo supervisado. Debe seleccionar al menos una opción de "Activar modo supervisado" o "Permitir la eliminación del perfil de MDM".
   - Obligatorio: si esta opción está seleccionada, a los usuarios no se les solicita que acepten la configuración de inscripción
   - Permitir la eliminación del perfil de MDM: si esta opción está seleccionada, los usuarios pueden desactivar los dispositivos. Debe seleccionar al menos una opción de "Activar modo supervisado" o "Permitir la eliminación del perfil de MDM".
   - Espere hasta que se haya realizado la configuración del dispositivo: si esta opción está seleccionada, los usuarios no pueden cancelar la configuración del dispositivo hasta que la activación con BlackBerry UEM haya finalizado. Esta configuración solo es válida si selecciona la opción "Activar modo supervisado".
9. En la sección **Omitir durante la configuración**, seleccione los elementos que no desea incluir en la instalación del dispositivo:
   - Código de acceso: si esta opción está seleccionada, a los usuarios no se les solicita que creen un código de acceso del dispositivo
   - Servicios de ubicación: si esta opción está seleccionada, los servicios de ubicación se desactivan en el dispositivo
   - Restaurar: si esta opción está seleccionada, los usuarios no pueden restaurar datos de un archivo de copia de seguridad
   - Mover desde Android: si esta opción está seleccionada, los usuarios no pueden restaurar los datos desde un dispositivo Android
   - ID de Apple: si esta opción está seleccionada, los usuarios no pueden iniciar sesión en ID de Apple y iCloud
   - Términos y condiciones: si esta opción está seleccionada, los usuarios no ven los términos y condiciones de iOS
   - Siri: si esta opción está seleccionada, Siri se desactiva en los dispositivos
   - Diagnóstico: si esta opción está seleccionada, la información de diagnóstico no se envía automáticamente desde el dispositivo durante la instalación
   - Biométrico: si esta opción está seleccionada, los usuarios no pueden configurar Touch ID
   - Pago: si esta opción está seleccionada, los usuarios no pueden configurar Apple Pay
   - Zoom: si esta opción está seleccionada, los usuarios no pueden configurar zoom
   - Configuración del botón de inicio: cuando está seleccionado, los usuarios no pueden ajustar el clic del botón de inicio
10. Haga clic en **Guardar**.
11. Si ha seleccionado "Asignar automáticamente los nuevos dispositivos a esta configuración", haga clic en **Sí**.

Después de terminar: Si no ha seleccionado "Asignar automáticamente los nuevos dispositivos a esta configuración", consulte Asignación de una configuración de inscripción a dispositivos iOS.

Eliminación de una configuración de inscripción que se ha asignado a los dispositivos iOS

Si se asignó una configuración de inscripción a los dispositivos y todavía no se ha aplicado, puede eliminarla de los dispositivos.

1. En la barra de menú, haga clic en **Usuarios > Dispositivos de Apple DEP**.
2. Seleccione las casillas de verificación situadas junto a los dispositivos de los que desea eliminar una configuración de inscripción. Debe seleccionar dispositivos que estén registrados a la misma cuenta de DEP.
3. Haga clic en .

4. Haga clic en **Eliminar**.

Después de terminar: Asignación de una configuración de inscripción a dispositivos iOS.

Eliminación de una configuración de inscripción

Si elimina una configuración de inscripción que está asignada a los dispositivos antes de aplicar dicha configuración, BlackBerry UEM elimina la configuración de inscripción asignada a los registros de dispositivo.

1. En la barra de menú, haga clic en **Configuración**.
2. En el panel izquierdo, haga clic en **Integración externa > Programa de inscripción de dispositivos de Apple**.
3. Haga clic en el nombre de una cuenta de DEP.
4. En la sección **Configuraciones de inscripción de DEP**, haga clic en ✕.
5. Haga clic en **Eliminar**.

Después de terminar: Si BlackBerry UEM elimina la configuración de inscripción desde los dispositivos, asigne dicha configuración a los dispositivos.

Cambio de los ajustes en una configuración de inscripción

Si se asignó una configuración de inscripción a los dispositivos y todavía no se ha aplicado, BlackBerry UEM la actualizará cuando guarde los cambios en la configuración.

1. En la barra de menús, haga clic en **Configuración**.
2. En el panel izquierdo, haga clic en **Integración externa > Programa de inscripción de dispositivos de Apple**.
3. Haga clic en el nombre de una cuenta de DEP.
4. En la sección **Configuraciones de inscripción de DEP**, haga clic en el nombre de la configuración que desea cambiar.
5. Cambie los ajustes.
6. Haga clic en **Guardar**.

Presentación de los ajustes de una configuración de inscripción que está asignada a un dispositivo

Si una configuración de inscripción está asignada a un dispositivo iOS y está pendiente, puede ver los ajustes de la configuración de la inscripción.

1. En la barra de menú, haga clic en **Usuarios > Dispositivos de Apple DEP**.
2. En la columna **Configuración de inscripción**, haga clic en el nombre de una configuración de inscripción.

Presentación de los datos de usuario para un dispositivo activado

Una vez que el dispositivo se haya activado correctamente, puede ver los detalles asociados con el usuario, como los grupos a los que está asignado.

1. En la barra de menú, haga clic en **Usuarios > Dispositivos de Apple DEP**.
2. En la columna **Nombre para mostrar**, haga clic en el nombre para mostrar de un usuario.

Activación de dispositivos iOS mediante Apple Configurator 2

Puede utilizar Apple Configurator 2 para preparar dispositivos iOS para la activación en BlackBerry UEM. Los usuarios pueden activar dispositivos preparados sin utilizar la aplicación BlackBerry UEM Client. Solo se requiere su nombre de usuario y la contraseña de activación.

Cuando los dispositivos están activados, BlackBerry UEM envía los perfiles y la política de TI que ha asignado a los usuarios en los dispositivos.

Nota: Para que funcionen determinadas funciones, debe asignar la aplicación BlackBerry UEM Client a los usuarios. Los usuarios deben iniciar BlackBerry UEM Client después de activar el dispositivo. Para obtener más información sobre cuándo debe asignar la aplicación BlackBerry UEM Client a los usuarios, visite support.blackberry.com/kb/ para leer el artículo KB39313.

Pasos para activar los dispositivos con Apple Configurator 2

Paso	Acción
1	También puede agregar la aplicación de BlackBerry UEM Client a la lista de aplicaciones y asignarla a las cuentas de usuario o a los grupos de usuarios. Consulte Adición de una aplicación de iOS a la lista de aplicaciones.
2	Adición de información del servidor de BlackBerry UEM a Apple Configurator 2.
3	Preparación de dispositivos iOS con Apple Configurator 2.
4	Cree un perfil de activación y asígnelo a una cuenta de usuario o a un grupo de usuarios.
5	Establezca una contraseña de activación y envíe un mensaje de correo de activación.
6	Distribuya los dispositivos a los usuarios y solicite que completen la instalación. Para aplicar un perfil de conformidad, los usuarios deben instalar y abrir la aplicación BlackBerry UEM Client una vez finalizada la configuración.

Adición de información del servidor de BlackBerry UEM a Apple Configurator 2

Antes de empezar: Descargue e instale la última versión de Apple Configurator 2 de Apple.

1. En el menú de Apple Configurator 2, seleccione **Preferencias > Servidores**.
2. Haga clic en + > **Siguiente**.
3. En el campo **Nombre**, escriba un nombre para el servidor.
4. En el campo**Nombre de host o URL**, escriba la URL del servidor de BlackBerry UEM con el siguiente formato:*<http o https>://<nombredeservidor>:<puerto>*; el puerto predeterminado es 8885. Para obtener más información acerca de la configuración de los puertos, consulte Puertos de escucha de BlackBerry UEM en el contenido de Instalación y actualización.
5. Haga clic en **Siguiente**.
6. Cierre la ventana **Servidor**.

Preparación de dispositivos iOS con Apple Configurator 2

Cuando prepare un dispositivo, Apple Configurator 2 borra el dispositivo y actualiza el sistema operativo del dispositivo a la versión más reciente.

Antes de empezar: Adición de información del servidor de BlackBerry UEM a Apple Configurator 2.

1. Abra Apple Configurator 2.
2. Conecte uno o más dispositivos iOS al equipo.
3. Haga clic en **Preparar**.
4. En la lista desplegable **Configuración**, seleccione **Manual**. Haga clic en **Siguiente**.
5. En la lista desplegable **Servidor**, seleccione el servidor de BlackBerry UEM. Haga clic en **Siguiente**.
6. De manera opcional, seleccione la casilla de verificación **Supervisar dispositivos**. Haga clic en **Siguiente**.
7. Si selecciona **Supervisar dispositivos**, complete la información de la empresa.
8. Haga clic en **Preparar** y espere a que el dispositivo esté preparado. El proceso puede tardar hasta 15 minutos.

Después de terminar: Distribuya los dispositivos a los usuarios para la activación.

Bloqueo de activación en los dispositivos iOS

La función de bloqueo de activación en dispositivos iOS permite a los usuarios proteger sus dispositivos si se pierden o se los roban. Cuando la función está activada, el usuario debe confirmar el ID y la contraseña de Apple ID para desactivar Buscar mi iPhone, borrar el dispositivo o reactivar y utilizar el dispositivo.

Para gestionar la función de bloqueo de activación en BlackBerry UEM:

- El dispositivo debe ser un dispositivo supervisado que ejecute iOS 7.1 o posterior.
- El dispositivo debe tener configurada una cuenta de iCloud.
- El dispositivo debe tener activada la opción Buscar mi iPhone o Buscar mi iPad.

Cuando se activa un dispositivo en BlackBerry UEM, el bloqueo de activación está desactivado de forma predeterminada. Puede activarlo para cada dispositivo de forma individual o puede forzar la activación utilizando la política de TI. Al activar el bloqueo de activación, BlackBerry UEM guarda un código de desvío que puede utilizar para borrar el bloqueo y que el dispositivo se pueda borrar y reactivar sin la contraseña ni el ID de Apple del usuario.

Conceptos relacionados

Activación de los dispositivos iOS que están inscritos en DEP

Activar bloqueo de activación

Complete los siguientes pasos para activar el bloqueo de activación para cada dispositivo de forma individual. Si se aplica forzosamente el bloqueo de activación utilizando una regla de política de TI, ya estará activado.

Nota: Al activar la función Bloqueo de activación, puede tener lugar una breve demora entre BlackBerry UEM y Apple.

Antes de empezar:

- El dispositivo debe ser un dispositivo supervisado que ejecute iOS 7.1 o posterior.
- El dispositivo debe tener configurada una cuenta de iCloud.
- El dispositivo debe tener activada la opción Buscar mi iPhone o Buscar mi iPad.

1. En la barra de menú, haga clic en **Usuarios**.
2. Busque una cuenta de usuario.
3. En los resultados de la búsqueda, haga clic en el nombre de la cuenta de usuario.
4. Haga clic en la pestaña del dispositivo.
5. En la ventana **Administrar dispositivo** haga clic en **Activar bloqueo de activación**.

Después de terminar: Para ver la lista de códigos de desvío para dispositivos, consulte Visualice el código de desvío del bloqueo de activación

Desactive bloqueo de activación

Complete los siguientes pasos para desactivar el bloqueo de activación para cada dispositivo de forma individual. Si se aplica forzosamente el bloqueo de activación utilizando una regla de política de TI, no podrá desactivarlo.

Nota: Al activar la función Bloqueo de activación, puede tener lugar una breve demora entre BlackBerry UEM y Apple.

1. En la barra de menú, haga clic en **Usuarios**.
2. Busque una cuenta de usuario.
3. En los resultados de la búsqueda, haga clic en el nombre de la cuenta de usuario.
4. Haga clic en la pestaña del dispositivo.
5. En la ventana **Administrar dispositivo**, seleccione **Desactivar bloqueo de activación**.

Visualice el código de desvío del bloqueo de activación

Puede ver el código de desvío del bloqueo de activación y la fecha en la que se generó dicho código.

1. En la barra de menú, haga clic en **Usuarios > Bloqueo de activación de Apple**.
2. Busque un dispositivo.
3. En los resultados de búsqueda, haga clic en el dispositivo.
4. Si es necesario, desplácese a la derecha de la pantalla principal para ver el código de desvío.

Activación de dispositivos BlackBerry 10 mediante BlackBerry Wired Activation Tool

BlackBerry Wired Activation Tool permite activar varios dispositivos BlackBerry 10 al mismo tiempo a través de conexiones USB en lugar de conexiones inalámbricas. Puede que la empresa desee usar este método por diferentes razones:

- Para hacer más rápida y fácil la activación de varios dispositivos a la vez
- Para mantener el proceso de activación en manos de los administradores
- Para activar los dispositivos y configurar las características de seguridad, tales como los requisitos de cifrado de contenido y perfiles VPN, antes de dárselos a los usuarios o conectarlos a la red de la empresa

No se pueden asignar perfiles y políticas mediante BlackBerry Wired Activation Tool. Debe asignar los perfiles y las políticas a los usuarios en la consola de gestión de BlackBerry UEM antes de asignar y activar dispositivos mediante BlackBerry Wired Activation Tool. Sin embargo, no es necesario establecer contraseñas de activación para asignar y activar dispositivos mediante BlackBerry Wired Activation Tool.

Para activar dispositivos mediante BlackBerry Wired Activation Tool, los dispositivos deben estar ejecutando BlackBerry 10 OS versión 10.3 o una versión posterior.

Puede descargar BlackBerry Wired Activation Tool aquí: Docs.blackberry.com/BES12tools

Configuración de BlackBerry Wired Activation Tool e inicio de sesión en una instancia de BlackBerry UEM

Antes de poder activar dispositivos con BlackBerry Wired Activation Tool, debe crear una configuración para cada instancia de BlackBerry UEM a la que necesite tener acceso. Después de crear una configuración, también debe utilizar una cuenta de administrador para permitir a BlackBerry Wired Activation Tool el acceso a BlackBerry Web Services.

1. En la carpeta de instalación de BlackBerry Wired Activation Tool, haga doble clic en el archivo **BWAT.exe**.
2. En **Agregar una pantalla de servidor de BES12**, en el campo **Nombre**, escriba un nombre para identificar la configuración que se va a crear. Por ejemplo, si tiene dos instancias de BlackBerry UEM, puede crear una configuración para cada una y darles un nombre, como Servidor 1 y Servidor 2.
3. En el campo **URL de BlackBerry Web Services**, escriba la dirección para el componente de BlackBerry Web Services. La dirección predeterminada es https://*<dirección web de BlackBerry UEM>*:18084.

   El puerto se puede cambiar modificando el ajuste `tomcat.bws.port` en la base de datos de BlackBerry UEM.
4. En el campo **URL de extremo BCP**, escriba la dirección que se debe utilizar para las activaciones de dispositivos. Esto también se conoce como URL de activación o Nombre del servidor. La dirección predeterminada es: http://*nombre.servidor*:8882/*ID_SRP*/mdm.

   Se puede encontrar la dirección asegurándose de que la variable %ActivationURL% está en la Plantilla del correo de activación y haciendo clic en **Ver correo electrónico de activación** desde cualquier pantalla de resumen de usuario.

   Si es necesario, también puede buscar la dirección del host y el puerto en la base de datos de BlackBerry UEM. En la tabla `def_cfg_setting_dfn`, busque los valores `id_setting_definition` de `bdmi.enroll.bcp.host` y `bdmi.enroll.bcp.port`. A continuación, utilice los valores `id_setting_definition` para buscar los valores de los ajustes en `obj_global_cfg_Setting`.
5. Haga clic en **Enviar**.
6. En la pantalla **Iniciar sesión**, seleccione una configuración de BlackBerry UEM de la lista desplegable.
7. En el campo **Nombre de usuario**, escriba el nombre de usuario de una cuenta de usuario de BlackBerry UEM con permisos de administrador.
8. En el campo **Contraseña**, escriba la contraseña de la cuenta.
9. En la lista desplegable **Directorio**, seleccione un método de autenticación.
10. Si es necesario, en el campo **Dominio**, escriba el dominio de Microsoft Active Directory.
11. Haga clic en **Iniciar sesión**.

Active los dispositivos BlackBerry 10 mediante BlackBerry Wired Activation Tool

Antes de empezar:

- Configure BlackBerry Wired Activation Tool e inicie sesión en una instancia de BlackBerry UEM.
- Encienda todos los dispositivos conectados y asegúrese de que, o todos los dispositivos han terminado el proceso de configuración inicial, o no lo han iniciado. No puede activar los dispositivos si el proceso de configuración inicial está en curso.

1. Conecte uno o más dispositivos BlackBerry 10 al equipo mediante cables USB.
2. Verifique la columna de **Estado** para cada dispositivo. Lleve a cabo una de las siguientes acciones:
   - Si en la columna Estado aparece **Requiere contraseña**, haga clic en **Requiere contraseña** para introducir la contraseña para el dispositivo
   - Si en la columna Estado aparece **Dispositivo no compatible**, actualice el software del dispositivo a BlackBerry 10 OS versión 10.3 o una versión posterior
   - Si en la columna Estado aparece **Preparado**, asigne el dispositivo a un usuario

3. En el campo **Buscar**, busque una cuenta de usuario a la que desea asignar un dispositivo.
4. En la lista de resultados de la búsqueda, haga clic en la cuenta de usuario.
5. En la sección principal de la pantalla, haga clic en un nombre de cuenta de usuario y arrastre el nombre hacia un dispositivo para asignar el dispositivo a dicho usuario. Repita el paso para asignar los dispositivos a varios usuarios.
6. Seleccione la casilla de verificación situada junto a los pares de usuarios y dispositivos que desea activar.
7. Haga clic en **Activar dispositivos**.

BlackBerry Wired Activation Tool activa todos los dispositivos seleccionados. Consulte la columna Estado para ver el progreso y los resultados de cada dispositivo. Si la activación no se completa, haga clic en el mensaje que aparece en la columna Estado para obtener más información acerca de los errores.

Sugerencias para la resolución de problemas de la activación del dispositivo

Cuando solucione problemas de activación de cualquier tipo de dispositivo, compruebe siempre lo siguiente:

- Asegúrese de que BlackBerry UEM sea compatible con el tipo de dispositivo. Para obtener más información acerca de los tipos de dispositivos compatibles, consulte la Matriz de compatibilidad.
- Asegúrese de que haya licencias disponibles para el tipo de dispositivo que el usuario activa y el tipo de activación que se asigna al usuario. Para obtener más información, consulte el contenido referente a Licencias.
- Compruebe la conectividad de red en el dispositivo.
  - Verifique que el móvil o la red Wi-Fi esté activa y tenga cobertura suficiente.
  - Si el usuario debe configurar manualmente una VPN o un perfil de Wi-Fi de trabajo para acceder a contenido detrás del firewall de la empresa, asegúrese de que los perfiles de usuario estén configurados correctamente en el dispositivo.
  - Si se trata de la red Wi-Fi de trabajo, asegúrese de que la ruta de red del dispositivo esté disponible. Para obtener más información acerca de la configuración de los firewalls de red para trabajar con BlackBerry UEM, visite http://support.blackberry.com/kb y lea el artículo 36470.
- Asegúrese de que el perfil de activación asignado permita activar el tipo de dispositivo.
- Si el dispositivo está intentando conectar con BlackBerry UEM o BlackBerry Infrastructure a través de un firewall de la empresa, verifique que los puertos del firewall adecuado estén abiertos. Para obtener más información acerca de los puertos necesarios, consulte el contenido referente a Instalación y actualización
- Recopilar registros del dispositivo:
  - Para obtener más información acerca de la recuperación de los archivos de registro del dispositivo con BlackBerry 10, visite http://support.blackberry.com/kb y lea el artículo 26038.

    Nota: Los archivos de registro del dispositivo BlackBerry 10 están cifrados. Para utilizar los archivos de registro del dispositivo BlackBerry 10 a efectos de resolución de problemas, debe tener una incidencia abierta con BlackBerry Technical Support Services. Únicamente los agentes de soporte técnico pueden descifrar los archivos de registro.
  - Para obtener más información acerca de la recuperación de los archivos de registro del dispositivo con iOS, visite http://support.blackberry.com/kb y lea el artículo 36986.
  - Para obtener más información acerca de la recuperación de los archivos de registro del dispositivo con Android, visite http://support.blackberry.com/kb y lea el artículo 32516.
  - Para obtener más información acerca de la recuperación de los registros de dispositivos Windows Phone, visite http://support.blackberry.com/kb y lea el artículo 36984.

Dispositivos KNOX Workspace y Android con un perfil de trabajo

Cuando solucione el problema de la activación de los dispositivos Samsung que utilizan Samsung KNOX Workspace, compruebe lo siguiente:

- Asegúrese de que el dispositivo sea compatible con KNOX Workspace. Consulte la información de Samsung.
- Asegúrese de que el bit de garantía no se haya activado. Consulte la información de Samsung.
- Asegúrese de que la versión del contenedor de KNOX sea compatible. KNOX Workspace requiere KNOX Container 2.0 o una versión posterior. Para obtener más información sobre las versiones de Samsung KNOX compatibles, consulte la lista de Samsung.

Cuando solucione el problema de la activación de los dispositivos Android con un perfil de trabajo, compruebe lo siguiente:

- Asegúrese de que el dispositivo es compatible con los perfiles de trabajo de Android. Para obtener más información, visite https://support.google.com/work/android/answer/6174145 y lea el artículo 6174145.
- Asegúrese de que haya una licencia disponible y de que el tipo de activación se establezca en Trabajo y personal: privacidad de usuario.
- Para utilizar el tipo de activación de Trabajo y personal: privacidad de usuario, los dispositivos deben estar ejecutando Android OS versión 5.1 o una versión posterior.
- Asegúrese de que la cuenta de usuario en BlackBerry UEM tenga la misma dirección de correo que la del dominio de Google. Si las direcciones de correo no coinciden, el dispositivo mostrará el siguiente error: no se puede activar el dispositivo - tipo de activación no compatible. Busque lo siguiente en el archivo de registro principal:
  - ```
    ERROR AfW: no se ha podido encontrar el usuario en el dominio de Google.
     Cancelando la creación y activación de usuarios.
    ```
  - ```
    ERROR marcado para cuarentena debido a: No se puede activar el dispositivo -
     Tipo de activación no admitido
    ```

No se puede completar la activación del dispositivo porque el servidor no tiene más licencias. Para obtener ayuda, contacte con el administrador.

Descripción

Este error se muestra en un dispositivo durante la activación cuando las licencias ya no están disponibles o han caducado.

Solución posible

En BlackBerry UEM, realice las acciones siguientes:

- Compruebe que las licencias estén disponibles para admitir la activación.
- Si es necesario, active las licencias o adquiera licencias adicionales.

Para obtener más información, consulte el contenido referente a Licencias.

Compruebe el nombre de usuario y la contraseña e inténtelo de nuevo.

Descripción

Este error se muestra en un dispositivo durante la activación cuando el usuario ha introducido un nombre de usuario o una contraseña incorrecta o ambas cosas.

Solución posible

Introduzca el nombre de usuario y la contraseña correctos.

Error de instalación del perfil. No se ha podido importar el certificado "AutoMDMCert.pfx".

Descripción

Este error se muestra en un dispositivo iOS durante la activación cuando ya existe un perfil en el dispositivo.

Solución posible

Vaya a **Configuración > General > Perfiles** en el dispositivo y compruebe que el perfil ya existe. Elimine el perfil y reactívelo. Si el problema persiste, es posible que tenga que reiniciar el dispositivo porque los datos podrían almacenarse en la memoria caché.

Error 3007: el servidor no está disponible

Descripción

El error puede aparecer en el dispositivo durante la activación debido a lo siguiente:

- El certificado que BlackBerry UEM utiliza para firmar el perfil de MDM que envía a los dispositivos iOS no es de confianza para el dispositivo. Al activar el dispositivo, se pide al usuario que confíe en este certificado.
- Si configura un proxy transparente como Blue Coat y supervisa el puerto 443 para tráfico no estándar, BlackBerry UEM Client no puede enviar los comandos CONEXIÓN HTTP y OPCIONES HTTP a BlackBerry UEM.

Soluciones posibles

Las soluciones posibles incluyen:

- Instale el certificado raíz para la autoridad de certificación que emita el certificado que utiliza BlackBerry UEM para firmar el perfil de MDM para el dispositivo iOS. Para obtener más información sobre este certificado, consulte el contenido de Configuración.
- Compruebe que la configuración de proxy no está bloqueando que BlackBerry UEM Client envíe los comandos CONEXIÓN HTTP y OPCIONES HTTP a BlackBerry UEM. Para obtener más información, visite http://support.blackberry.com/kb y lea el artículo 38644.

No se puede contactar con el servidor, compruebe la conectividad o la dirección del servidor

Descripción

El error puede aparecer en el dispositivo durante la activación debido a lo siguiente:

- Se ha introducido de forma incorrecta el nombre de usuario en el dispositivo.
- Se ha introducido de forma incorrecta la dirección del cliente para la activación del dispositivo en el dispositivo.

  Nota: Esto solo es necesario cuando el registro con BlackBerry Infrastructure ha sido desactivado.
- No se ha establecido la contraseña de activación o esta ha caducado.

Soluciones posibles

Las soluciones posibles incluyen:

- Verificar el nombre de usuario y la contraseña.
- Verificar la dirección del cliente para la activación del dispositivo.
- Definir una nueva contraseña de activación mediante BlackBerry UEM Self-Service.

iOS or macOS device activations fail with an invalid APNs certificate

Causa posible

Si no puede activar dispositivosiOSomacOS, el certificado APN podría no estar correctamente registrado.

Solución posible

Lleve a cabo una o más de las siguientes acciones:

- En la consola de gestión, en la barra de menú, haga clic en **Configuración > Integración externa > Apple Push Notification**. Compruebe que el estado de certificado de APN es "Instalado". Si el estado no es correcto, intente volver a registrar el certificado de APN.
- Para probar la conexión entre BlackBerry UEM y el servidor de APN, haga clic en **Probar certificado APN**.
- Si es necesario, obtenga una nueva CSR firmada de BlackBerry y solicite y registre un nuevo certificado APN.

Los usuarios no reciben el correo de activación

Descripción

Los usuarios no reciben el correo de activación, aunque todos los ajustes en BlackBerry UEM son correctos.

Solución posible

Si los usuarios utilizan un servidor de correo de terceros, los mensajes de correo procedentes de BlackBerry UEM se pueden marcar como no deseados y terminar en la carpeta de correo no deseado.

Asegúrese de que los usuarios hayan verificado la carpeta de correo no deseado para buscar el correo de activación.

Comandos y controles del dispositivo

BlackBerry UEM le permite enviar comandos a los dispositivos a través de la red inalámbrica para proteger los datos del dispositivo. También puede ubicar los dispositivos en un mapa y controlar los dispositivos que tienen acceso a Exchange ActiveSync.

Envío de comandos para los usuarios y dispositivos

Puede enviar varios comandos a través de la red inalámbrica para gestionar las cuentas y los dispositivos de los usuarios. La lista de comandos que están disponibles depende del tipo de dispositivo y el tipo de activación. Puede enviar comandos a un usuario o dispositivo específico, o bien enviar comandos a varios usuarios y dispositivos mediante comandos masivos.

Por ejemplo, puede utilizar los comandos en las siguientes circunstancias:

- Si un dispositivo se pierde temporalmente, puede enviar un comando para bloquear el dispositivo o eliminar los datos de trabajo del dispositivo.
- Si desea redistribuir un dispositivo a otro usuario en la empresa, o si un dispositivo se pierde o se roba, puede enviar un comando para eliminar todos los datos del dispositivo.
- Cuando un empleado deja la empresa, puede enviar un comando al dispositivo personal del usuario para eliminar solo los datos de trabajo.
- Si un usuario olvida la contraseña del espacio de trabajo, puede enviar un comando para restablecer la contraseña del espacio de trabajo.
- Para los usuarios con dispositivos supervisados de DEP, puede enviar un comando para activar una actualización del SO.

Enviar un comando a un dispositivo

Antes de empezar:

Si desea establecer un periodo de caducidad para los comandos que eliminan datos de los dispositivos de BlackBerry UEM, consulte Establecer un tiempo de caducidad para comandos.

1. En la barra de menú, haga clic en **Usuarios > Dispositivos gestionados**.
2. Busque una cuenta de usuario.
3. En los resultados de la búsqueda, haga clic en el nombre de la cuenta de usuario.
4. Haga clic en la pestaña del dispositivo.
5. En la ventana **Gestionar dispositivo**, seleccione el comando que desee enviar al dispositivo.

Envío de un comando masivo

Puede enviar un comando a varias cuentas de usuario o dispositivos al mismo tiempo seleccionando los usuarios o dispositivos en la lista de usuarios y enviando un comando masivo.

Antes de empezar: Si desea establecer un periodo de caducidad para los comandos que eliminan datos de los dispositivos, consulte Establecer un tiempo de caducidad para comandos.

1. En la barra de menú, haga clic en **Usuarios > Dispositivos gestionados**.
2. Si fuera necesario, filtre la lista de usuarios.
3. Lleve a cabo una de las siguientes acciones:
   - Seleccione la casilla para marcar en la parte superior de la lista de usuarios para seleccionar todos los usuarios y dispositivos de la lista.

- Seleccione la casilla para marcar correspondiente a los usuarios y dispositivos que desea incluir. Puede utilizar Mayús+clic para seleccionar varios usuarios.

4. En el menú, haga clic en uno de los siguientes iconos:

Icono	Descripción
	Ubicar dispositivos Puede seleccionar un máximo de 100 dispositivos cada vez. Para obtener más información, consulte Ubicar un dispositivo.
	Enviar correo Para obtener más información, consulte Envío de un correo a los usuarios.
	Enviar correo de activación Para obtener más información, consulte Envío de un mensaje de correo electrónico de activación a varios usuarios.
	Agregar a grupos de usuarios Puede seleccionar un máximo de 200 dispositivos cada vez. Para obtener más información, consulte Agregar usuarios a los grupos de usuarios.
	Exportar Para obtener más información, consulte Exportación de la lista de usuarios a un archivo .csv .
	Eliminar dispositivos Para utilizar este comando masivo, debe ser un administrador de seguridad. Puede seleccionar un máximo de 200 dispositivos cada vez. Para obtener más información, consulte Comandos para todos los tipos de dispositivos.
	Actualizar la información del dispositivo. Para obtener más información, consulte Comandos para todos los tipos de dispositivos.
	Eliminar todos los datos del dispositivo Para utilizar este comando, debe ser un administrador de seguridad. Puede seleccionar un máximo de 200 dispositivos cada vez. Este comando masivo no es compatible con dispositivos macOS. Para obtener más información, consulte Referencia de comandos.
	Eliminar solo los datos de trabajo Para utilizar este comando, debe ser un administrador de seguridad. Puede seleccionar un máximo de 200 dispositivos cada vez. Para obtener más información, consulte Referencia de comandos.

Icono	Descripción
	Editar propiedad del dispositivo Puede seleccionar un máximo de 100 dispositivos cada vez. Para obtener más información, consulte Cambio de la etiqueta de la propiedad de dispositivo.
	Actualizar SO Puede forzar los dispositivos iOS supervisados para instalar una actualización del SO. Para utilizar este comando, debe ser un administrador de seguridad. Puede seleccionar un máximo de 200 dispositivos cada vez. Para obtener más información, consulte Actualización del SO en dispositivos de iOS supervisados.
	Cambiar contraseñas de la consola Puede enviar una contraseña de BlackBerry UEM Self-Service a varios usuarios al mismo tiempo. Para obtener más información, consulte Enviar una contraseña de BlackBerry UEM Self-Service a varios usuarios.

Establecer un tiempo de caducidad para comandos

Cuando envía el comando "Eliminar todos los datos del dispositivo" o "Eliminar solo los datos de trabajo" a un dispositivo, este debe conectarse a BlackBerry UEM para que el comando se complete. Si el dispositivo no se puede conectar a BlackBerry UEM, el comando permanece en estado pendiente y el dispositivo no se elimina de BlackBerry UEM a menos que se elimine manualmente. Opcionalmente, se puede configurar BlackBerry UEM para que elimine automáticamente los dispositivos cuando no se completan los mandos tras un tiempo especificado.

1. En la barra de menú, haga clic en **Configuración > Configuración general > Caducidad del comando Eliminar**.
2. Para una o ambas opciones **Eliminar todos los datos del dispositivo** y **Eliminar solo los datos de trabajo**, seleccione **Eliminar automáticamente el dispositivo si el comando no se ha completado**.
3. En el campo **Caducidad del comando**, indique tras cuántos días desea que caduque el comando y se elimine automáticamente el dispositivo de BlackBerry UEM.
4. Haga clic en **Save (Guardar)**.

Referencia de comandos

Los comandos que puede enviar a los dispositivos varían en función de los tipos de dispositivo y activación. Algunos comandos se pueden enviar a varios dispositivos a la vez.

Comandos para todos los tipos de dispositivos

Comando	Descripción
Actualizar la información del dispositivo	Este comando envía y recibe información del dispositivo actualizada. Por ejemplo, puede enviar reglas de políticas de TI actualizadas recientemente o perfiles a un dispositivo y recibir información actualizada acerca de un dispositivo, como la versión del SO o el nivel de la batería. Para dispositivos macOS, el comando es "Actualizar datos de escritorio". Para dispositivos Windows 10, el comando envía una solicitud al dispositivo para crear una solicitud de validación del certificado de estado. El dispositivo envía la solicitud al Servicio de atestación de mantenimiento de Microsoft para comprobar la conformidad. Para enviar este comando a varios dispositivos, consulteEnvío de un comando masivo.
Ver acciones de dispositivo	Este comando muestra todas las acciones que están en curso en un dispositivo. Para obtener más información, consulte Presentación de las acciones de dispositivo.
Ver informe del dispositivo	Este comando muestra información detallada acerca de un dispositivo. Puede exportar y guardar el informe del dispositivo en el equipo. Para obtener más información, consulte Ver y guardar un informe de dispositivo.
Eliminar dispositivo	Este comando elimina el dispositivo de BlackBerry UEM. El dispositivo puede seguir recibiendo correos electrónicos y otros datos de trabajo. Para enviar este comando a varios dispositivos, consulteEnvío de un comando masivo.

Comandos para dispositivos Android

Comando	Descripción	Tipos de activación
Eliminar todos los datos del dispositivo	Este comando elimina toda la información del usuario y los datos de aplicaciones que almacena el dispositivo, incluida la información en el espacio de trabajo, y devuelve el dispositivo a la configuración predeterminada de fábrica. Si el dispositivo no se puede conectar a BlackBerry UEM cuando envía este comando, puede cancelar el comando o eliminar el dispositivo de la consola. Si el dispositivo se conecta a BlackBerry UEM una vez que lo elimine, solo se eliminarán los datos de trabajo del dispositivo, incluido el espacio de trabajo, si procede. Para enviar este comando a varios dispositivos, consulteEnvío de un comando masivo.	• Controles de MDM • Trabajo y personal: control total (Samsung KNOX) • Solo espacio de trabajo - (Samsung KNOX)

Comando	Descripción	Tipos de activación
Eliminar solo los datos de trabajo	Este comando elimina datos de trabajo, incluida la política de TI, los perfiles, las aplicaciones y los certificados que se encuentran en el dispositivo y desactiva el dispositivo. Si el dispositivo tiene un espacio de trabajo, la información del espacio de trabajo y el espacio de trabajo se eliminan del dispositivo. Para obtener más información, consulte Desactivación de dispositivos. Si el dispositivo no se puede conectar a BlackBerry UEM cuando envía este comando, puede cancelar el comando o eliminar el dispositivo de la consola. Si el dispositivo se conecta a BlackBerry UEM una vez que lo haya eliminado, se eliminarán los datos de trabajo del dispositivo, incluido el espacio de trabajo, si procede. Para enviar este comando a varios dispositivos, consulteEnvío de un comando masivo.	• Todas (excepto BlackBerry 2FA)
Bloquear dispositivo	Este comando bloquea el dispositivo. El usuario debe escribir la contraseña del dispositivo para desbloquear el dispositivo. Si un dispositivo se pierde de manera temporal, puede utilizar este comando. Cuando se envía este comando, el dispositivo se bloquea solo si existe una contraseña para el dispositivo. De lo contrario, no se realiza ninguna acción en el dispositivo.	• Controles de MDM • Trabajo y personal: control total (Samsung KNOX) • Trabajo y personal: privacidad de usuario • Trabajo y personal: privacidad de usuario (Premium) • Solo espacio de trabajo • Solo espacio de trabajo (Premium)
Desbloquear dispositivo y borrar contraseña	Este comando desbloquea el dispositivo y solicita al usuario que cree una nueva contraseña para el dispositivo. Si el usuario omite la pantalla "Crear contraseña de dispositivo" se conserva la contraseña anterior. Puede utilizar este comando si un usuario olvida la contraseña del dispositivo. **Nota:** Este comando no es compatible en los dispositivos que no sean Samsung, ejecuten Android 7.0 o posterior y se hayan activado con Controles de MDM.	• Controles de MDM • Trabajo y personal: control total (Samsung KNOX) • Trabajo y personal: privacidad de usuario (Samsung KNOX)

Comando	Descripción	Tipos de activación
Especificar la contraseña del dispositivo y bloquearlo	Este comando permite crear una contraseña del dispositivo y, a continuación, bloquear el dispositivo. Debe crear una contraseña que cumpla con las actuales reglas para la contraseña. Para desbloquear el dispositivo, el usuario debe escribir la nueva contraseña. **Nota:** Este comando no es compatible en los dispositivos que no sean Samsung que ejecuten Android 7.0 y posterior y que se hayan activado con Controles de MDM. **Nota:** Para los tipos de activación Trabajo y personal: privacidad de usuario, solo los dispositivos BlackBerry con Android 8.x o posterior son compatibles con este comando.	• Controles de MDM • Trabajo y personal: control total (Samsung KNOX) • Solo espacio de trabajo • Solo espacio de trabajo (Premium) • Trabajo y personal: privacidad de usuario • Trabajo y personal: privacidad de usuario (Premium)
Restablecer contraseña del espacio de trabajo	Este comando elimina la contraseña actual del espacio de trabajo del dispositivo. Cuando el usuario abre el espacio de trabajo, el dispositivo solicita al usuario que defina una nueva contraseña del espacio de trabajo.	• Trabajo y personal: control total (Samsung KNOX) • Trabajo y personal: privacidad de usuario - (Samsung KNOX) • Solo espacio de trabajo - (Samsung KNOX)
Especificar contraseña de espacio de trabajo y bloquear	Para los dispositivos Android versión 7.0 o posterior, puede especificar una contraseña del espacio de trabajo y bloquear el dispositivo. Cuando el usuario abre una aplicación de perfil de trabajo Android, debe introducir la contraseña que se especificó.	• Trabajo y personal: privacidad de usuario • Trabajo y personal: privacidad de usuario (Premium)
Desactivar/activar espacio de trabajo	Este comando desactiva o activa el acceso a las aplicaciones del espacio de trabajo en el dispositivo.	• Trabajo y personal: control total (Samsung KNOX) • Trabajo y personal: privacidad de usuario - (Samsung KNOX) • Solo espacio de trabajo - (Samsung KNOX)
Desactivar BlackBerry 2FA	Este comando desactiva los dispositivos que se activan con el tipo de activación BlackBerry 2FA. El dispositivo se elimina de BlackBerry UEM y el usuario no puede utilizar la característica BlackBerry 2FA.	• BlackBerry 2FA
Limpiar aplicaciones	Este comando borra los datos de todas las aplicaciones gestionadas por Microsoft Intune en el dispositivo. Las aplicaciones no se eliminan del dispositivo. Para obtener más información, consulte Borrar aplicaciones gestionadas por Microsoft Intune	• Todas (excepto BlackBerry 2FA)

Comandos para dispositivos iOS

Comando	Descripción	Tipos de activación
Eliminar todos los datos del dispositivo	Este comando elimina toda la información de usuario y los datos de aplicaciones que el dispositivo guarda y devuelve el dispositivo a la configuración predeterminada de fábrica. Si el dispositivo no se puede conectar a BlackBerry UEM cuando envía este comando, puede cancelar el comando o eliminar el dispositivo de la consola. Si el dispositivo se conecta a BlackBerry UEM una vez que lo elimine, solo se eliminarán los datos de trabajo del dispositivo. Para enviar este comando a varios dispositivos, consulteEnvío de un comando masivo.	• Controles de MDM
Eliminar solo los datos de trabajo	Este comando elimina datos de trabajo, incluidas las políticas de TI, los perfiles, las aplicaciones y los certificados que se encuentran en un dispositivo. Si el dispositivo no se puede conectar a BlackBerry UEM cuando envía este comando, puede cancelar el comando o eliminar el dispositivo de la consola. Si el dispositivo se conecta a BlackBerry UEM una vez que lo elimine, se eliminarán los datos de trabajo del dispositivo. Para enviar este comando a varios dispositivos, consulteEnvío de un comando masivo.	• Controles de MDM • Privacidad del usuario
Bloquear dispositivo	Este comando bloquea un dispositivo. El usuario debe escribir la contraseña del dispositivo para desbloquear el dispositivo. Si un dispositivo se pierde de manera temporal, puede utilizar este comando. Cuando se envía este comando, el dispositivo se bloquea solo si existe una contraseña para el dispositivo. De lo contrario, no se realiza ninguna acción en el dispositivo. Este comando no es compatible con dispositivos Apple TV.	• Controles de MDM
Desbloquear y borrar contraseña	Este comando desbloquea un dispositivo y elimina la contraseña. Al usuario se le indica que cree una contraseña para el dispositivo. Puede utilizar este comando si el usuario olvida la contraseña del dispositivo. Este comando no es compatible con dispositivos Apple TV.	• Controles de MDM

Comando	Descripción	Tipos de activación
Activar modo perdido	Este comando bloquea el dispositivo y le permite establecer un número de teléfono y un mensaje que se mostrará en el dispositivo. Por ejemplo, puede mostrar la información de contacto cuando se encuentre el dispositivo. Después de enviar este comando, podrá ver la ubicación del dispositivo desde BlackBerry UEM. Este comando es compatible con los dispositivos iOS supervisados con iOS 9.3 o posterior. Este comando no es compatible con dispositivos Apple TV.	• Controles de MDM
Desactivar BlackBerry 2FA	Este comando desactiva los dispositivos que se activan con el tipo de activación "BlackBerry 2FA ". El dispositivo se elimina de BlackBerry UEM y el usuario no puede utilizar la característica BlackBerry 2FA. Este comando no es compatible con dispositivos Apple TV.	• BlackBerry 2FA
Actualizar SO	Este comando fuerza a los dispositivos a instalar una actualización del SO. Es compatible con los siguientes dispositivos: • dispositivos supervisados que ejecutan iOS 10.3 y posterior • dispositivos DEP supervisados que ejecutan iOS 9.0 y posterior Para obtener más información, consulte Actualización del SO en dispositivos de iOS supervisados. Para enviar este comando a varios dispositivos, consulte Envío de un comando masivo. Este comando no es compatible con dispositivos Apple TV.	• Controles de MDM
Reiniciar dispositivo	Este comando fuerza a los dispositivos a reiniciarse. Compatible con los dispositivos iOS supervisados que ejecutan 10.3 o posterior. Este comando no es compatible con dispositivos Apple TV.	• Controles de MDM
Desactivar dispositivo	Este comando fuerza a los dispositivos a desactivarse. Compatible con los dispositivos iOS supervisados que ejecutan 10.3 o posterior. Este comando no es compatible con dispositivos Apple TV.	• Controles de MDM

Comando	Descripción	Tipos de activación
Limpiar aplicaciones	Este comando borra los datos de todas las aplicaciones gestionadas por Microsoft Intune en el dispositivo. Las aplicaciones no se eliminan del dispositivo. Para obtener más información, consulte Borrar aplicaciones gestionadas por Microsoft Intune	• Controles de MDM

Comandos para dispositivos macOS

Comando	Descripción	Tipos de activación
Bloquear escritorio	Este comando le permite establecer un PIN y bloquear el dispositivo.	• Controles de MDM
Eliminar solo los datos de trabajo	Este comando elimina datos de trabajo, incluida la política de TI, los perfiles, aplicaciones y certificados que se encuentran en el dispositivo y opcionalmente, elimina el dispositivo de BlackBerry UEM. Para enviar este comando a varios dispositivos, consulteEnvío de un comando masivo.	• Controles de MDM
Eliminar todos los datos del dispositivo	Este comando elimina toda la información del usuario y los datos de aplicaciones del dispositivo. Devuelve el dispositivo a los valores predeterminados de fábrica, lo bloquea con el PIN que establezca y, opcionalmente, elimina el dispositivo de BlackBerry UEM. No se admite como un comando masivo.	• Controles de MDM

Comandos para dispositivos BlackBerry 10

Comando	Descripción	Tipos de activación
Especificar contraseña de dispositivo, bloquear y establecer mensaje	Este comando permite crear una contraseña del dispositivo y configurar un mensaje de la pantalla de inicio y, a continuación, bloquea el dispositivo. Debe crear una contraseña que cumpla con las actuales reglas para la contraseña. Cuando el usuario desbloquea el dispositivo, el dispositivo solicita al usuario que acepte o rechace la contraseña nueva. Si una política de TI requiere que el dispositivo tenga la misma contraseña para el dispositivo y el espacio de trabajo, este comando también cambia la contraseña del espacio de trabajo.	• Trabajo y personal - Empresa • Solo espacio de trabajo • Trabajo y personal - Regulado

Comando	Descripción	Tipos de activación
Eliminar todos los datos del dispositivo	Este comando elimina toda la información del usuario y los datos de las aplicaciones que guarda el dispositivo, incluida la información del espacio de trabajo. Devuelve el dispositivo a la configuración predeterminada de fábrica y, de manera opcional, elimina el dispositivo de BlackBerry UEM. Si el dispositivo no se puede conectar a BlackBerry UEM cuando envía este comando, puede cancelar el comando o eliminar el dispositivo de la consola. Si el dispositivo se conecta a BlackBerry UEM una vez que lo elimine, solo se eliminarán los datos de trabajo del dispositivo. Para enviar este comando a varios dispositivos, consulteEnvío de un comando masivo.	• Trabajo y personal - Empresa • Solo espacio de trabajo • Trabajo y personal - Regulado
Especificar contraseña de espacio de trabajo y bloquear	Este comando permite crear una contraseña del espacio de trabajo en el dispositivo y bloquear el espacio de trabajo. Debe crear una contraseña que cumpla con las actuales reglas para la contraseña. Para desbloquear el espacio de trabajo, el usuario debe escribir la nueva contraseña que cree. Si una política de TI requiere que el dispositivo tenga la misma contraseña para el dispositivo y el espacio de trabajo, este comando también cambia la contraseña del dispositivo.	• Trabajo y personal - Empresa • Trabajo y personal - Regulado
Eliminar solo los datos de trabajo	Este comando elimina datos de trabajo, incluida la política de TI, los perfiles, aplicaciones y certificados que se encuentran en el dispositivo y opcionalmente, elimina el dispositivo de BlackBerry UEM. Si el dispositivo tiene un espacio de trabajo, la información del espacio de trabajo se elimina y el espacio de trabajo se elimina del dispositivo. Si el dispositivo no se puede conectar a BlackBerry UEM cuando envía este comando, puede cancelar el comando o eliminar el dispositivo de la consola. Si el dispositivo se conecta a BlackBerry UEM una vez que lo elimine, se eliminarán los datos de trabajo del dispositivo. Para enviar este comando a varios dispositivos, consulteEnvío de un comando masivo.	• Trabajo y personal - Empresa • Trabajo y personal - Regulado

Comandos para dispositivos Windows

Comando	Descripción	Tipos de activación
Bloquear dispositivo	Este comando bloquea un dispositivo. El usuario debe escribir la contraseña del dispositivo para desbloquear el dispositivo. Si un dispositivo se pierde de manera temporal, puede utilizar este comando. Cuando se envía este comando, el dispositivo se bloquea solo si existe una contraseña para el dispositivo. De lo contrario, no se realiza ninguna acción en el dispositivo. Este comando es compatible con los dispositivos con Windows 10 Mobile y Windows Phone 8.1 o posterior.	Controles de MDM
Generar contraseña de dispositivo y bloquear	Este comando crea una contraseña del dispositivo y bloquea el dispositivo. La contraseña generada se envía al usuario por correo. Puede utilizar la dirección de correo preseleccionada, o especificar una dirección de correo. La contraseña generada cumple con las reglas para la contraseña. Este comando es compatible solo con los dispositivos con Windows 10 Mobile y el SO Windows Phone versión 8.10.14176 o posterior.	Controles de MDM
Eliminar solo los datos de trabajo	Este comando elimina datos de trabajo, incluida la política de TI, los perfiles, aplicaciones y certificados que se encuentran en el dispositivo y opcionalmente, elimina el dispositivo de BlackBerry UEM. La cuenta de usuario no se elimina al enviar este comando. Después de enviar este comando, se le dará la opción de eliminar el dispositivo de BlackBerry UEM. Si el dispositivo no se puede conectar a BlackBerry UEM, puede eliminar el dispositivo de BlackBerry UEM. Si el dispositivo se conecta a BlackBerry UEM una vez que lo haya eliminado, solo se eliminarán los datos de trabajo del dispositivo, incluido el espacio de trabajo, si procede. Para enviar este comando a varios dispositivos, consulteEnvío de un comando masivo.	Controles de MDM

Comando	Descripción	Tipos de activación
Eliminar todos los datos del dispositivo	Este comando elimina toda la información del usuario y los datos de aplicaciones guardados en el dispositivo. Devuelve el dispositivo a los valores predeterminados de fábrica y opcionalmente, elimina el dispositivo de BlackBerry UEM. Después de enviar este comando, se le dará la opción de eliminar el dispositivo de BlackBerry UEM. Si el dispositivo no se puede conectar a BlackBerry UEM, puede eliminar el dispositivo de BlackBerry UEM. Si el dispositivo se conecta a BlackBerry UEM una vez que lo haya eliminado, solo se eliminarán los datos de trabajo del dispositivo, incluido el espacio de trabajo, si procede. Para enviar este comando a varios dispositivos, consulteEnvío de un comando masivo.	Controles de MDM
Reinicie el escritorio o dispositivo	Este comando fuerza a los dispositivos a reiniciarse. Este comando solo es compatible con dispositivos Windows 10.	Controles de MDM

Comandos para dispositivos con BlackBerry OS (de la versión 5.0 a 7.1)

BlackBerry OS (versión 5.0 a 7.1)

Comando	Descripción
Especificar la contraseña del dispositivo y bloquearlo	Este comando permite crear una contraseña del dispositivo, a continuación, bloquea el dispositivo. Debe crear una contraseña que cumpla con las actuales reglas para la contraseña. Si usted o un usuario ha activado la protección del contenido de dos factores, no podrá utilizar este comando.
Eliminar solo los datos de trabajo	Este comando elimina los datos de trabajo, incluida la política de TI, los mensajes de correo, los contactos y los libros de servicio del trabajo que están en el dispositivo. Todos los datos personales permanecen en el dispositivo.
Eliminar todos los datos del dispositivo	Este comando elimina permanentemente toda la información de usuario y los datos de aplicaciones que el dispositivo guarda y devuelve el dispositivo a los valores predeterminados de fábrica. Puede enviar este comando a un dispositivo que desee distribuir a otro usuario o a un dispositivo que se haya perdido y que el usuario podría no recuperar.
Volver a enviar los libros de servicios	Este comando vuelve a enviar los libros de servicio a un dispositivo. Los libros de servicio especifican qué servicios están disponibles en un dispositivo BlackBerry OS.
Volver a enviar política de TI	Este comando vuelve a enviar la política de TI de BlackBerry OS asignada a un dispositivo.

Desactivación de dispositivos

Cuando usted o un usuario desactiva el dispositivo, la conexión entre el dispositivo y la cuenta de usuario en BlackBerry UEM se elimina. No se puede gestionar el dispositivo y ya no aparece en la consola de gestión. El usuario no puede acceder a los datos de trabajo en el dispositivo.

Puede desactivar un dispositivo mediante el comando "Eliminar solo los datos de trabajo". Los usuarios pueden desactivar los dispositivos a través de los siguientes métodos:

- Para dispositivos iOS, Android o Windows Phone, los usuarios pueden seleccionar "Desactivar mi dispositivo" en la pantalla "Acerca de" en la aplicación BlackBerry UEM Client.
- Para los dispositivos Windows 10, los usuarios pueden seleccionar Configuración > Cuentas > Acceso de trabajo > Eliminar.
- Para los dispositivos BlackBerry 10, los usuarios pueden seleccionar Configuración > BlackBerry Balance > Eliminar espacio de trabajo.

Para los dispositivos que usan KNOX MDM, cuando el dispositivo está desactivado, se desinstalan las aplicaciones internas y la opción de desinstalación está disponible para cualquier aplicación pública que se haya instalado desde la lista de aplicaciones según sea necesario.

Para los dispositivos con perfil de trabajo Android con Solo espacio de trabajo, si desactiva un dispositivo, puede eliminar todos los datos de la tarjeta SD y eliminar la protección de restablecimiento de fábrica.

En los dispositivos Samsung KNOX Workspace que se han activado mediante los tipos de activación Trabajo y personal: control total o Solo espacio de trabajo, al desactivar el dispositivo se eliminan todos los datos del dispositivo o solo del espacio de trabajo. Puede especificar los datos que se borran utilizando la regla de política de TI "Borrado de datos durante la desactivación".

Ubicar un dispositivo

Puede localizar dispositivos iOS, Android y Windows 10 Mobile (por ejemplo, si se extravía o se roba un dispositivo). Los usuarios deben aceptar el perfil de servicio de ubicación con anterioridad para que la consola de gestión muestre las ubicaciones de los dispositivos iOS y Android en un mapa. Los dispositivos Windows 10 Mobile aceptan automáticamente el perfil. El historial de ubicaciones está disponible para dispositivos iOS y Android si lo ha activado en el perfil.

Antes de empezar: Cree y asigne un perfil de servicio de ubicación.

1. En la barra de menú, haga clic en **Usuarios > Dispositivos gestionados**.
2. Seleccione la casilla de verificación correspondiente a los dispositivos que desea ubicar.
3. Haga clic en .
4. Encuentre los dispositivos en el mapa con los siguientes iconos. Si un dispositivo iOS o Android no responde con la última información de ubicación y el historial de ubicaciones está activado en el perfil, el mapa muestra la última ubicación conocida del dispositivo.
   - Ubicación actual:
   - Última ubicación conocida:

   Puede hacer clic o desplazar el cursor sobre un icono para mostrar la información de ubicación, como latitud y longitud, y cuándo se informó de la ubicación (por ejemplo, hace un minuto o hace dos horas).
5. Para ver el historial de ubicaciones de un dispositivo iOS o Android, realice las siguientes acciones:
   a) Haga clic en **Ver historial de ubicaciones**.
   b) Seleccione un intervalo de fecha u hora.

c) Haga clic en **Enviar**.

Tareas relacionadas

Creación de un perfil de servicio de ubicación

Uso del modo perdido para dispositivos iOS supervisados

Puede activar y gestionar el modo perdido para dispositivos iOS supervisados con iOS 9.3 o posterior. Si se pierde un dispositivo, la activación del modo perdido le permite:

- Bloquear el dispositivo y establecer el mensaje que desea mostrar (por ejemplo, puede mostrar la información de contacto para cuando alguien encuentre el dispositivo).
- Ver la ubicación actual del dispositivo sin necesidad de utilizar un perfil de servicio de ubicación.
- Controlar todos los dispositivos que se encuentren en el modo perdido desde la consola de gestión.

Activar modo perdido

El modo perdido es compatible con los dispositivos supervisados iOS con iOS 9.3 o posterior.

1. En la barra de menú, haga clic en **Usuarios > Dispositivos gestionados**.
2. Haga clic en el dispositivo para el desea activar el modo perdido.
3. En la pestaña Dispositivo, haga clic en **Activar modo perdido**.
4. En los campos **Número de teléfono de contacto** y **Mensaje**, escriba la información correspondiente.
5. De manera opcional, seleccione **Sustituir diapositiva para desbloquear texto** e introduzca el texto para mostrar.
6. Haga clic en **Activar**.

Localización de un dispositivo en modo perdido

Antes de empezar: Activar modo perdido

1. En la barra de menú, haga clic en **Usuarios > Dispositivos gestionados**.
2. Haga clic en un dispositivo que tiene el modo perdido activado.
3. En la pestaña Dispositivo, haga clic en **Obtener ubicación del dispositivo**.

Desactivar modo perdido

Antes de empezar: Activar modo perdido

1. En la barra de menú, haga clic en **Usuarios > Dispositivos gestionados**.
2. Haga clic en un dispositivo que tiene el modo perdido activado.
3. En la pestaña Dispositivo, haga clic en **Desactivar modo perdido**.

Vea las actualizaciones disponibles para dispositivos iOS

Puede ver si hay una actualización de software disponible para los dispositivos iOS de sus usuarios, de forma que puedan actualizar el software a la versión más reciente.

1. En la barra de menú, haga clic en **Usuarios > Dispositivos gestionados**.
2. Busque una cuenta de usuario.

3. En los resultados de la búsqueda, haga clic en el nombre de la cuenta de usuario.
4. Seleccione la pestaña dispositivo.
5. En la sección de dispositivo Activado, consulte si hay una actualización disponible.

Tareas relacionadas

Envío de un correo a los usuarios

Restricción de los dispositivos iOS sin supervisión

Hay dos maneras para restringir los dispositivos iOS sin supervisión en BlackBerry UEM:

- Para los dispositivos que están inscritos en DEP, puede asignar una configuración de inscripción a los que tienen el ajuste "Activar modo supervisado" seleccionado. Cuando los dispositivos se activen, se activarán automáticamente en modo supervisado. Para obtener más información, consulte Asignación de una configuración de inscripción a dispositivos iOS.
- Puede asignar un perfil de activación que tenga el ajuste "No permitir activar dispositivos no supervisados" seleccionado para las cuentas de usuario. Este ajuste es compatible con los tipos de activación "Controles MDM" y "Privacidad del usuario" (con licencias basadas en SIM activadas). BlackBerry UEM impide que los dispositivos no supervisados se activen y elimina automáticamente los dispositivos si se quedan sin supervisión, aunque se hayan activado con BlackBerry UEM Client o mediante DEP. Para obtener más información, consulte Creación de un perfil de activación.

Actualización del SO en dispositivos de iOS supervisados

Puede forzar los dispositivos siguientes para instalar una actualización del SO:

- dispositivos supervisados que ejecutan iOS 10.3 y posterior
- dispositivos DEP supervisados que ejecutan iOS 9.0 y posterior

Para actualizar el SO en varios dispositivos, consulte Envío de un comando masivo.

1. En la barra de menú, haga clic en **Usuarios > Dispositivos gestionados**.
2. Busque una cuenta de usuario.
3. En los resultados de la búsqueda, haga clic en el nombre de la cuenta de usuario.
4. Haga clic en la pestaña del dispositivo.
5. En el panel izquierdo, si hay una actualización de software disponible, haga clic en **Actualizar ahora**.
6. En la lista desplegable, seleccione una de las opciones siguientes:
   - **Descargar e instalar**: la actualización se descarga e instala automáticamente en el dispositivo.
   - **Solo descarga**: la actualización se descarga automáticamente en el dispositivo y se le solicita al usuario que la instale.
   - **Instalar las actualizaciones descargadas**: si la actualización ya se ha descargado en un dispositivo, se instala automáticamente.
7. Haga clic en **Submit**.

Creación de mensajes de ayuda del dispositivo

En los dispositivos con Android 8.0 y versiones posteriores, puede crear un mensaje de ayuda que se muestra en el dispositivo cuando una función se desactiva debido a una política de TI. El mensaje se muestra en la pantalla de configuración para la función que está desactivada. Si no crea un mensaje de ayuda, el dispositivo muestra el mensaje predeterminado del sistema operativo.

También puede especificar un mensaje de ayuda de administrador que se muestra en la pantalla de configuración Administraciones del dispositivo. Por ejemplo, puede que desee mostrar un aviso de que su empresa puede supervisar y gestionar aplicaciones y datos en el perfil de trabajo.

Si su empresa cuenta con usuarios que trabajan en más de un idioma, puede agregar mensajes de ayuda en idiomas adicionales y especificar el idioma predeterminado que se muestra en los dispositivos que no utilizan uno de los idiomas disponibles.

Crear mensajes de ayuda del dispositivo

Los mensajes de ayuda del dispositivo son compatibles con dispositivos con Android 8.0 y versiones posteriores.

1. En la barra de menú, haga clic en **Configuración > Configuración general**.
2. Haga clic en **Mensajes de ayuda del dispositivo personalizados**.
3. En la pestaña **Mensajes de ayuda del dispositivo personalizados**, haga clic en **Agregar**.
4. Seleccione el idioma en el que desea que aparezca la notificación.
5. En el campo **Aviso de funciones desactivada**, escriba el aviso que desea mostrar en el dispositivo cuando una función está desactivada. El mensaje puede tener hasta 200 caracteres.
6. Opcionalmente, en el campo **Mensaje de ayuda de administrador**, escriba un aviso para que se muestre en la pantalla de configuración Administradores del dispositivo.
7. Si desea crear un mensaje en más de un idioma, haga clic en **Agregar un idioma adicional** y repita los pasos del 4 al 6 para cada idioma.
8. Si ha agregado mensajes en más de un idioma, seleccione **Idioma predeterminado** junto al idioma que desea que aparezca en los dispositivos que no utilizan uno de los idiomas disponibles. Por ejemplo, si los idiomas disponibles son inglés y francés, e inglés es el idioma predeterminado, el mensaje en inglés parecerá en los dispositivos que utilicen alemán.
9. Haga clic en **Guardar**.

Permiso para que los usuarios de BlackBerry 10 realicen copias de seguridad de los datos del dispositivo

Puede controlar si los usuarios de BlackBerry 10 pueden realizar copias de seguridad de los datos del dispositivo y restaurarlos. Puede permitir a los usuarios realizar copias de seguridad solo de los datos del espacio personal o de los datos del espacio tanto personal como de trabajo. En la política de TI que asigne a los usuarios puede seleccionar una de las siguientes reglas de políticas de TI o ambas:

Regla de política de TI	Tipos de activación aplicables
Permitir copia de seguridad y restauración del dispositivo	• Trabajo y personal - Regulado • Solo espacio de trabajo

Regla de política de TI	Tipos de activación aplicables
Permitir copia de seguridad y restauración del espacio de trabajo	• Trabajo y personal - Empresa • Trabajo y personal - Regulado **Nota:** Para dispositivos activados con "Trabajo y personal - Regulado", esta regla se aplica solo si se ha seleccionado la regla "Permitir copia de seguridad y restauración del dispositivo".

Si la política de TI que se ha asignado a los usuarios permite copias de seguridad del dispositivo, los usuarios pueden iniciar sesión en BlackBerry Link para crear o restaurar archivos de copia de seguridad.

Cuando los usuarios crean archivos de copia de seguridad mediante BlackBerry Link, los archivos se cifran mediante claves de cifrado que BlackBerry UEM envía a los dispositivos con BlackBerry 10. Las claves de cifrado iniciales se generan cuando se instala o se actualiza a BlackBerry UEM versión 12.4. Si es necesario, puede generar nuevas claves de cifrado, importar claves de cifrado desde otra instancia de BlackBerry UEM o exportar claves de cifrado.

Generación de claves de cifrado

Puede generar las claves de cifrado que se utilizan para cifrar los archivos de copia de seguridad cuando los usuarios realizan una copia de seguridad de los datos de sus dispositivos con BlackBerry 10. Las claves de cifrado iniciales se generan automáticamente cuando se instala o se actualiza a BlackBerry UEM versión 12.4.

1. En la barra de menú, haga clic en **Configuración > Configuración general > Copia de seguridad y restauración de BB10**.
2. Haga clic en **Generar nueva clave**.
3. Haga clic en **Generar**.

Después de terminar: Las claves de cifrado se envían a todos los dispositivos con BlackBerry 10 que estén activados en BlackBerry UEM.

Exportación de claves de cifrado

Puede exportar las claves de cifrado de BlackBerry UEM para poderlas importar en otra instancia de BlackBerry UEM.

1. En la barra de menú, haga clic en **Configuración > Configuración general > Copia de seguridad y restauración de BB10**.
2. Haga clic en **Exportar claves**.
3. Escriba y confirme una contraseña para el archivo.
4. Haga clic en **Exportar**.
5. Guarde el archivo.

Importación de claves de cifrado

Puede importar claves de cifrado en BlackBerry UEM que se hayan generado y exportado desde otra instancia de BlackBerry UEM.

Antes de empezar: Verifique que dispone de la contraseña del archivo de claves de cifrado que va a importar.

1. En la barra de menú, haga clic en **Configuración > Configuración general > Copia de seguridad y restauración de BB10**.
2. Haga clic en **Importar claves**.
3. Haga clic en **Examinar** y navegue hasta el archivo de claves de cifrado. Haga clic en **Abrir**.

4. Escriba la contraseña del archivo.
5. Haga clic en **Importar**.

Eliminación de claves de cifrado

Cuando genera una nueva clave de cifrado, las claves generadas previamente solo resultan útiles para el descifrado. Si ya no necesita claves generadas previamente, puede eliminarlas de BlackBerry UEM. La clave de cifrado generada más recientemente no se puede eliminar.

1. En la barra de menú, haga clic en **Configuración > Configuración general > Copia de seguridad y restauración de BB10**.
2. Para eliminar una clave de cifrado, junto a la clave, haga clic en ✕.
3. Para confirmar que desea eliminar permanentemente la clave, escriba "blackberry". Haga clic en **Eliminar**.

Mantenimiento, supervisión y creación de informes

Puede supervisar el estado de BlackBerry UEM mediante los archivos de registro, los archivos de registro de auditoría y las herramientas de SNMP, y puede generar informes a partir de el panel y la lista de usuarios.

Uso de archivos de registro

Puede utilizar los archivos de registro para identificar y solucionar problemas con los componentes o dispositivos BlackBerry UEM en el entorno de la empresa. Las capacidades de registro de BlackBerry UEM permiten:

- Realizar el seguimiento de la actividad de los componentes de BlackBerry UEM mediante los registros del servidor
- Enviar los datos del archivo de registro BlackBerry UEM a un servidor syslog o a un archivo de texto
- Recuperar archivos de registro de los dispositivos Android y con BlackBerry 10
- Auditar la actividad de aplicación en los dispositivos BlackBerry 10

Administración de archivos de registro BlackBerry UEM

El tamaño de los archivos de registro varía en función del número de usuarios y dispositivos del entorno de BlackBerry UEM y de su nivel de actividad. Se recomienda supervisar y controlar la cantidad de espacio que utilizan en el disco los archivos de registro. Para evitar que ocupen demasiado espacio de disco, puede especificar un tamaño máximo de archivo y el nivel de depuración de los archivos de registro.

Puede configurar los ajustes de registro en los siguientes niveles:

- Opciones de inicio de sesión global: estos ajustes se aplican a todas las instancias de BlackBerry UEM en la empresa que comparten la misma base de datos. Estos ajustes incluyen la ubicación del archivo syslog y el tamaño máximo de los archivos de registro.
- Opciones de inicio de sesión de instancia: estos ajustes se aplican únicamente a la instancia BlackBerry UEM que desea seleccionar y anulan la configuración general. Estos ajustes incluyen la activación de la opción de una ubicación local para los archivos de registro y el nivel de registro del archivo de registro.

Configurar opciones de inicio de sesión global

1. En la barra de menú, haga clic en **Configuración** > **Infraestructura** > **Registro**.
2. Configure las siguientes opciones generales como obligatorias para el entorno de la empresa:

   Nota: Los cambios de estos valores de configuración requieren que se reinicie el sistema.

Configuración	Pasos
Para enrutar los eventos del sistema a un servidor syslog	**a.** Seleccione la casilla de verificación de **Reg. sistema**. De forma predeterminada, esta casilla de verificación no está seleccionada. **b.** Especifique el nombre del host y el puerto del servidor syslog donde desea enrutar los eventos de registro de BlackBerry UEM.
Para poder especificar una ubicación en la instancia del servidor donde se almacenan los archivos de registro del componente de BlackBerry UEM	**a.** Seleccione la casilla de verificación **Activar destino de archivo local**.

Configuración	Pasos
Para activar el registro avanzado de la comunicación entre servidor y dispositivo para la resolución de problemas	**a.** Seleccione la casilla de verificación **Activar registro de carga de MDM**.
Para establecer un límite de tamaño máximo para los archivos de registro de componentes de BlackBerry UEM	En el campo **Tamaño máximo de archivo de registro**, especifique el tamaño máximo en MB que cada archivo de registro puede alcanzar. Cuando un archivo de registro alcanza el tamaño máximo, BlackBerry UEM inicia una nueva instancia del archivo de registro.
Para establecer la antigüedad máxima del archivo de registro del servidor de los archivos de registro del componente de BlackBerry UEM	En el campo **Antigüedad máxima del archivo de registro del servidor**, especifique el número máximo de días que desea conservar los archivos de registro del servidor antes de que se eliminen. Si no especifica un valor, los archivos de registro no se eliminarán.
Para especificar una ruta de destino de red para los archivos de registro de los dispositivos con Android y BlackBerry 10	En el campo **Ubicación de la red de registro del dispositivo**, especifique la ruta UNC donde desea guardar los archivos de registro de actividad que recupere de los dispositivos mediante la consola de gestión.
Antigüedad máxima del archivo de registro de la auditoría de la aplicación del dispositivo	En el campo **Antigüedad máxima del archivo de registro de la auditoría de la aplicación del dispositivo**, especifique el número máximo de días que desea conservar los archivos de registro de la auditoría de las aplicaciones del dispositivo antes de que se eliminen. Si no especifica un valor, los archivos de registro no se eliminarán.

3. Haga clic en **Guardar**.

Establecer un nivel de registro para componente de BlackBerry UEM individuales

Para ayudar en la resolución de problemas y evitar que el rendimiento se vea afectado por el exceso de generación de archivos de registro, puede activar componentes de BlackBerry UEM individuales para que se escriban en los archivos de registro en diferentes niveles de información. Por ejemplo, puede configurar BlackBerry UEM Core para generar archivos de registro en el nivel de depuración y dejar el resto de los componentes para generar archivos de registro en el nivel de información.

1. En la barra de menú, haga clic en **Configuración > Infraestructura > Registro**.
2. Amplíe **Opciones de inicio de sesión global**.
3. En la sección **Omisión de registro de servicio**, haz clic en +.
4. Seleccione un componente de UEM.
5. En la lista desplegable **Nivel de registro**, seleccione un nivel de registro.
6. Haga clic en **Guardar**.

Después de terminar: Si es necesario, puede anular esta configuración. Para obtener más información, consulte Cambiar la configuración predeterminada para instancias de BlackBerry Connectivity Node y Crear un grupo de servidores.

Configuración de opciones de inicio de sesión de instancia

1. En la barra de menú, haga clic en **Configuración** > **Infraestructura** > **Registro**.
2. Amplíe la instancia del servidor que desea configurar.
3. Configure las siguientes opciones como obligatorias para el entorno de la empresa:

Configuración	Pasos
Para especificar la ubicación donde se guardan los archivos de registro del componente de BlackBerry UEM	**Nota:** Debe seleccionar la casilla de verificación **Activar destino de archivo local** en la configuración de registro global para que pueda cambiar la configuración. **a.** En el campo **Ruta del registro de servidor**, escriba la ruta donde desea guardar los archivos de registro de servidor. De forma predeterminada, los archivos de registro se guardan en `C:\Program Files\BlackBerry\UEM\Logs\`*`aaaammdd`*.
Para establecer el nivel de detalle incluido en los archivos de registro	En la lista desplegable **Niveles de depuración de registros**, seleccione una de las acciones siguientes: • **Información**: escribir los mensajes de actividades diarias, advertencia y error en el archivo de registro. • **Advertencia**: escribir los mensajes de advertencia y error en el archivo de registro. Los mensajes de advertencia son eventos inesperados que pueden requerir que tome medidas. • **Error**: escribir todos los mensajes de error en el archivo de registro. Cuando aparece una condición de error, normalmente debe realizar alguna acción. • **Depuración**: escribir información requerida únicamente para depurar un problema. • **Seguimiento**: escribir información adicional que un desarrollador puede utilizar para la depuración. De forma predeterminada el nivel de depuración se establece en **Información**.
Para especificar la carpeta para los archivos de registro de auditoría de la aplicación de dispositivos Android y con BlackBerry 10	En el campo **Ruta del registro de auditoría de la aplicación del dispositivo**, escriba la ruta donde desea guardar los archivos de registro de la auditoría de la aplicación.
Para establecer un límite de tamaño máximo para los archivos de registro de la auditoría de la aplicación del dispositivo	En el campo **Tamaño máximo de registro de auditoría de la aplicación**, especifique el tamaño máximo en MB que puede alcanzar el registro de auditoría de la aplicación del dispositivo. Cuando un archivo de registro alcanza el tamaño máximo, BlackBerry UEM inicia una nueva instancia del archivo de registro.

4. Haga clic en **Guardar**.

Modificación de la antigüedad máxima para un archivo de registro

1. En la barra de menú, haga clic en **Configuración** > **Infraestructura** > **Registro**.

2. Amplíe **Opciones de inicio de sesión global**.
3. Configure la antigüedad máxima del archivo de registro del servidor en días.
4. Haga clic en **Guardar**.

Cambiar el nivel de registro a Advertir para clientes Microsoft Intune

Si usa Microsoft Intune, debe cambiar el nivel de registro a Advertir.

1. En el servidor BlackBerry UEM para el que desea cambiar el nivel de registro, busque el archivo log4J.xml. La ubicación predeterminada del archivo es `C:\Archivos de programa\BlackBerry\BES\Core\tomcat-core\webapps\ROOT\WEB-INF\classes`
2. En el archivo, antes del valor <root>, agregue la siguiente información: `<logger name="org.apache.http.wire"> <level value="warn"/> </logger>`
3. Reinicie el servicio de BlackBerry UEM Core.

Búsqueda de archivos de registro

De forma predeterminada, un archivo de registro de un servidor se crea para cada componente de BlackBerry UEM y se guarda diariamente en el equipo donde se ha instalado el componente. Si instala varias instancias de BlackBerry UEM, cada equipo crea sus propios archivos de registro. BlackBerry UEM pone nombre a los archivos de registro *<server_name>_<component_identifier>_<yyyymmdd>_<log_number>.<file extension>* (por ejemplo, BBServer01_MDAT_20140730_0001.txt).

Los siguientes archivos de registro están disponibles en una solución BlackBerry UEM:

- Archivos de registro de componentes que se utilizan para administrar los dispositivos con BlackBerry 10, iOS, Android y Windows.

  Los archivos de registro son:

  - ACCS - archivos de registro de acceso de Tomcat
  - AFMGR - archivos de registro de BlackBerry Affinity Manager
  - BGS - archivos de registro de BlackBerry Gatekeeping Service
  - BSG - archivos de registro de BlackBerry Secure Gateway
  - CORE - archivos de registro de BlackBerry UEM Core
  - DISP - archivos de registro de BlackBerry Dispatcher
  - EVNT - archivos de registro de eventos de BlackBerry UEM Core
  - MDAT - archivos de registro de BlackBerry MDS Connection Service
  - TMCT - archivos de registro del servidor Tomcat
  - UI - archivos de registro de la consola de gestión de BlackBerry UEM
  - El archivo <Server_FQDN>_yyyymmdd.csv*<Computer_FQDN>*_yyyymmdd.csv utilizado para iniciar sesión en BlackBerry MDS Connection Service de BlackBerry UEM.

    Nota: Para obtener más información sobre el archivo de registro .csv de BlackBerry MDS Connection Service, visite support.blackberry.com/kb para consultar el artículo 36936.

  Los archivos de registro adicionales se crean cuando se instala por primera vez BlackBerry UEM.

  De forma predeterminada, estos archivos de registro se guardan en `<unidad>:\Program Files\BlackBerry\UEM\Logs\<fecha o nombre de carpeta>`
- Los archivos de registro que utiliza BlackBerry Secure Connect Plus son:

  - BSCP - archivos de registro de BlackBerry Secure Connect Plus que registran datos para las conexiones con la aplicación BlackBerry Secure Connect Plus
  - BSCP-TS - archivos de registro principales de BlackBerry Secure Connect Plus que registran los datos acerca del componente de BlackBerry Secure Connect Plus

Los archivos de registro de BlackBerry Secure Connect Plus se guardan en <unidad>:\Program Files \BlackBerry\UEM\Logs\.

- Los archivos de registro que utiliza BlackBerry Work Connect Notification Service son:
  - BWCN - archivos de registro BlackBerry Work Connect Notification Service

  Los archivos de registro de BlackBerry Work Connect Notification Service se guardan en `<unidad>:\Program Files\BlackBerry\UEM\Logs\BWCN\<nombre de archivo>`
- Los archivos de registro de componentes se utilizan para administrar dispositivos BlackBerry OS (de la versión 5.0 a la 7.1) (si procede)

  De forma predeterminada, los archivos de registro se guardan diariamente en `C:\Program Files \Research In Motion\BlackBerry Enterprise Server\Logs\<fecha o nombre de carpeta>`.

  Para obtener más información acerca de archivos de registro de BES5, consulte la Guía de administración de BES5.
- Los archivos de registro para los registros de BBM, los de llamadas, los de PIN a PIN, los de SMS/MMS y los de videochat se guardan en formato .csv y se utilizan para auditar la actividad de la aplicación.

  De forma predeterminada, los archivos de registro de auditoría de aplicaciones de los dispositivos BlackBerry 10 se guardan en *C:\Program Files\BlackBerry\UEM\Logs* y los archivos de registro de auditoría de aplicaciones de los dispositivos BlackBerry OS se guardan en *C:\Program Files (x86)\Research in Motion\BlackBerry Enterprise Server\Logs*.
- Los archivos de registro de Good Control se almacenan en: *C:\Program Files\BlackBerry\UEM\Logs\gclogs*
- Los archivos de registro de Good Proxy se almacenan en: *C:\Program Files\BlackBerry\UEM\Logs\gpslogs*

Lectura de los archivos de registro

Los archivos de registro de BlackBerry UEM se guardan en dos formatos, como valores separados por comas y como archivos de texto.

Los registros de BlackBerry Gatekeeping Service, los registros de paquetes de BlackBerry UEM, los registros de contactos y mensajes, de llamadas telefónicas, de PIN, de SMS y videochat de BlackBerry Messenger se guardan en formato CSV.

Todos los demás archivos de registro se guardan en formato TXT.

Lectura de los archivos de registro .csv

Los archivos de registro separados por comas contienen información diferente dependiendo del componente, el dispositivo o la aplicación de dispositivo para los que registren información. Algunos ejemplos de archivos de registro en formato .csv incluyen el archivo de registro de BlackBerry Gatekeeping Service y los archivos de la auditoría de la aplicación del dispositivo, como el BBM o el registro de llamadas telefónicas.

Puede identificar la información contenida en los archivos de registro .csv porque cada línea de registro presenta la información de una manera simple y consistente, por ejemplo, cada línea en el archivo de registro de SMS presentará la información en el siguiente formato:

```
Name.ID,"Email Address","Type of Message","To","From","Callback Phone
 Number","Body","Send/Received Date","Server Log Date","Overall Message
 Status","Command","UID"
```

Cada línea de un archivo de registro de teléfono, se presentaría en el siguiente formato:

```
Name.ID,"Type of Call","Name","Phone Number","Start Date","Server Log
 Date","Elapsed Time","Memo","Command","UID","Phone Line"
```

Lectura de los archivos de registro .txt

Los archivos de registro guardados como archivos .txt tienen dos formatos básicos:

- El primer formato es el más común y generalmente comienza con la fecha y la hora, proporcionando la información de la siguiente manera:

  ```
  TimeStamp Hostname AppName ProcessId MessageID [StructuredData] Message
  ```

  Por ejemplo:

  ```
  2015-06-12T12:07:17.634-0400 computer.example.com MDM localhost-startStop-1
   logging.feature.admin.application.management|logging.component.appmgmt
   [{{requestId,543ade23}{myContextInfo,runningContext}}] INFO  Total 2 routes,
   of which 2 is started.
  ```

- El segundo formato, que empieza con un indicador de nivel numérico, proporciona información de la siguiente manera:

  ```
  Level Date Thread CID Message
  ```

  Por ejemplo:

  ```
  <#03>[30000] (09/10 00:00:00.122):{0x520} [DIAG] EVENT=Thread_report,
   THREADID=0x1390, THREADNAME="SRPReceiverHandler"
  ```

Puede haber alguna variación basada en el componente o en la función que se está registrando, pero todos los archivos de registro que se guardan como archivos `.txt` contienen la siguiente información básica.

Elemento	Descripción
Fecha o marca de hora	Una marca de hora con la forma <Fecha><Hora><diferencia horaria respecto a UTC>. El campo Fecha/Hora indica la fecha y la hora de un evento en particular. **Nota:** La marca de fecha y de hora es la hora del servidor local.
El nombre de host o la identificación del componente	La identificación de componentes, o el nombre de host, indica para qué componente es el archivo de registro. En algunos casos, como CORE o MDS-CS, está claro. En otros en los que se utiliza un identificador numérico, no está tan claro
Nombre de la aplicación	El nombre de la aplicación es el mismo para todos los archivos de registro y aparece como MDM.
ID de proceso o subproceso	Representa el ID del subproceso de Java que actualmente está registrando un mensaje. Por ejemplo: `localhost-startStop-1`

Elemento	Descripción
ID de mensaje	El ID del mensaje identifica el tipo de mensaje que se envía al archivo de registro. Es una combinación de la función y el componente que se registra con el formato <función>|<componente>. Por ejemplo: `admin.application.management|appmgmt`
Datos estructurados	Cero o más pares de valores de nombre que representan datos estructurados. Por ejemplo: `[{{requestId,543ade23} {myContextInfo,runningContext}}]`
Mensaje	El mensaje indica la actividad y describe la naturaleza del evento. Un mensaje podría incluir información sobre el hardware o el software, o bien sobre el problema que se está produciendo. Por ejemplo: `INFO  Total 2 routes, of which 2 is started.`

Nivel	El nivel de evento indica el tipo de entrada de registro. Normalmente, los eventos encajarían en una de las categorías siguientes:
	• ERROR = Error
	• WARN = Advertencia
	• INFO = Información
	ENV = Entorno
	• DEBUG = Depuración
	• Otros
	  • DIAG = Diagnóstico
	  • TRAC = Seguimiento
	En algunos archivos de registro, el nivel aparece con un valor numérico, con el siguiente formato:
	• [10000] = Error
	• [20000] = Advertencia
	• [30000] = Información
	• [40000] = Depuración
	• [50000] = Otros

Niveles de archivo de registro

Nivel	Descripción
DEBUG	En este nivel se especifica la información que es útil para depurar problemas de codificación. Los eventos pueden incluir lo siguiente: • Estados de recursos sospechosos en condiciones de error • Transiciones entre los componentes internos y externos • REST envía solicitudes a BlackBerry UEM Core • Solicitudes a Microsoft Active Directory
ERROR	Este nivel especifica una condición de error que requiere que usted o un especialista de soporte técnico tome medidas. Los eventos pueden incluir lo siguiente: • Excepciones de codificación • Excepciones de nivel de datos • Excepciones de codificación recuperable
INFO	En este nivel se especifican eventos del sistema normales que los administradores o los especialistas de soporte técnico puede que deseen ver. Este nivel es el nivel de registro predeterminado de BlackBerry UEM.
TRACE	En este nivel se especifica la información que es útil para los que posean conocimientos de desarrollador, incluida la información que se utiliza para las clases y los métodos de seguimiento, los parámetros de método, etc.
WARN	En este nivel puede aparecer una condición de advertencia para la que podría ser necesario intervenir o bien un evento inesperado. Los eventos pueden incluir lo siguiente: • Datos incoherentes • Solicitudes inesperadas • Errores de autorización • Errores de autenticación

Uso de los archivos de registro para solucionar problemas

Identificador del componente	Componente de registro	Descripción
ACCS	Archivos de registro de acceso al servidor Apache Tomcat	Los archivos de registro de Apache Tomcat ACCS registran todas las solicitudes de acceso a los servicios web de BlackBerry UEM. Puede utilizar estos archivos de registro cuando desee comprobar el éxito o error de las solicitudes de acceso a los servicios web de BlackBerry UEM.

Identificador del componente	Componente de registro	Descripción
AFMGR	BlackBerry Affinity Manager	BlackBerry Affinity Manager contiene información sobre la funcionalidad y el estado de conmutación por error si tiene más de un BlackBerry Affinity Manager en el entorno de la empresa. También puede solucionar problemas relacionados con: • La conectividad entre BlackBerry UEM y BlackBerry Infrastructure • La conectividad entre BlackBerry UEM y los dispositivos BlackBerry 10 • Los problemas de estado que se originan al cambiar el BlackBerry Affinity Manager activo.
BGS	BlackBerry Gatekeeping Service	Puede utilizar estos archivos de registro cuando intente solucionar problemas con: • Los dispositivos que no se pueden activar en un entorno en el que BlackBerry Gatekeeping Service está en uso • La conectividad con su BlackBerry Gatekeeping Service • La conectividad entre BlackBerry UEM y BlackBerry Infrastructure • Las activaciones de BlackBerry 10 y el envío de las políticas y perfiles • La conectividad de iOS, Android y Windows Phone
BSCP	BlackBerry Secure Connect Plus	Registra datos sobre el componente de BlackBerry Secure Connect Plus. Puede utilizar estos archivos de registro para comprobar que BlackBerry Secure Connect Plus esté conectado a BlackBerry Infrastructure. Por ejemplo: 2015-01-19T13:17:47.540-0500 - BSCP {TcpClientConnectorNio#2} logging.feature.bscp.service| logging.component.bscp.pss.bcp [{}] - DEPURACIÓN Ping recibido desde [id: 0x60bce5a3, /192.0.2.0:28231 => bcp.example.com/192.0.2.124:3101], respuesta con Pong. 2015-01-19T13:18:22.989-0500 - BSCP {ChannelPinger#1} logging.feature.bscp.service| logging.component.bscp.pss.bcp [{}] - DEPURACIÓN enviando ping a [id: 0xb4a1677a, /192.0.2.0:28232 => bcp.example.com/192.0.2.124:3101]

Identificador del componente	Componente de registro	Descripción
BSCP-TS	BlackBerry Secure Connect Plus Core	Registra datos para las conexiones con el cliente BlackBerry Secure Connect Plus. Puede utilizar estos archivos de registro para comprobar que BlackBerry Secure Connect Plus esté preparado para recibir llamadas del cliente de BlackBerry Secure Connect Plus en los dispositivos. Por ejemplo: 47: [14:13:21.231312][][3][AsioTurnSocket-1] Conectado, host=68-171-243-141.rdns.blackberry.net 48: [14:13:21.239312][][3][AsioTurnSocket-1] Creando ubicación TURN 49: [14:13:21.405121][][3][AsioTurnSocket-1] asignación TURN creada Utilícelos para verificar que los dispositivos estén utilizando el túnel seguro. Por ejemplo: 74: [10:39:45.746926][][3][Tunnel-2FFEC51E] Sent: 2130.6 KB (1733), Received: 201.9 KB (1370), Running: 00:07:00.139249
BSG	BlackBerry Secure Gateway	Puede utilizar estos archivos de registro cuando intente solucionar problemas con: • Dispositivos iOS que no pueden enviar ni recibir mensajes de correo electrónico • La conectividad entre BlackBerry UEM y BlackBerry Infrastructure • Conectividad entre la BlackBerry Infrastructure y el servidor de correo Microsoft Exchange o Microsoft Office 365
BWCN	BlackBerry Work Connect Notification Service	Puede utilizar estos archivos de registro cuando se solucionan problemas con los dispositivos iOS que no están recibiendo notificaciones de elementos nuevos o modificados.
CORE	BlackBerry UEM Core	Puede utilizar estos archivos de registro cuando intente solucionar problemas con: • Los servicios o las transacciones principales • Transacciones BlackBerry 2FA • La migración de datos de BES10
DISP	BlackBerry Dispatcher	Puede utilizar estos archivos de registro cuando intente solucionar problemas con: • La conectividad entre BlackBerry UEM y BlackBerry Infrastructure • La conectividad entre BlackBerry UEM y los dispositivos BlackBerry 10

Identificador del componente	Componente de registro	Descripción
EVNT	BlackBerry UEM Core	Puede utilizar estos archivos de registro para encontrar notificaciones acerca de eventos específicos en BlackBerry UEM Core.
MDAT	BlackBerry MDS Connection Service	Puede utilizar estos archivos de registro cuando intente solucionar problemas con: • Las aplicaciones del dispositivo BlackBerry 10 • Los problemas de inserción de aplicaciones • Los problemas de autenticación de inserción de aplicaciones
ROUT	BlackBerry Router	Puede utilizar estos archivos de registro cuando intente solucionar problemas con: • La instalación de BlackBerry Router • La conectividad entre BlackBerry UEM y BlackBerry Router • La conectividad entre BlackBerry UEM y BlackBerry Infrastructure • La conectividad entre BlackBerry Router y BlackBerry Infrastructure • La conectividad entre dispositivos y BlackBerry UEM **Nota:** Los archivos de registro BlackBerry Router están disponibles solo si se ha instalado BlackBerry Router en el entorno de la empresa.
TMCT	Los archivos de registro del servidor Apache Tomcat	Los archivos de registro de Apache Tomcat TMCT registran todas las actividades de los servicios web de Apache Tomcat. Puede utilizar estos archivos de registro cuando existen problemas con la consola de gestión.
UI	Consola de administración	Puede utilizar estos archivos de registro cuando existen problemas con la consola de gestión.

La auditoría de la actividad de aplicación en BlackBerry 10 y BlackBerry OS dispositivos

Puede utilizar los registros del dispositivo para auditar la actividad de la aplicación en los dispositivos BlackBerry 10 con el tipo de activación "Trabajo y personal - Empresa", "Trabajo y personal - Regulado" y "Solo espacio de trabajo" y los dispositivos BlackBerry OS (de la versión 5.0 a la 7.1).

Debe configurar las siguientes reglas de políticas de TI para generar estos archivos de registro:

Las reglas de política de TI para BlackBerry 10	Las reglas de política de TI para los dispositivos BlackBerry OS	Descripción
Sincronizar los registros de BBM	Desactivar la sincronización inalámbrica de BlackBerry Messenger	La regla especifica si en un dispositivo se sincronizan registros de BlackBerry Messenger con BlackBerry UEM.
Sincronizar los registros del teléfono	Desactivar la sincronización inalámbrica del registro de llamadas telefónicas	La regla especifica si en un dispositivo se sincroniza el registro de llamadas de la aplicación de teléfono con BlackBerry UEM.
Sincronizar los registros PIN a PIN	Desactivar la sincronización inalámbrica de los mensajes PIN	Esta regla especifica si en un dispositivo se sincronizan los registros de mensajes PIN con BlackBerry UEM.
Sincronizar los registros SMS/MMS	Desactivar la sincronización inalámbrica de los mensajes SMS	Esta regla especifica si en un dispositivo se sincronizan los registros de mensajes de texto SMS y los mensajes MMS con BlackBerry UEM.
Sincronizar los registros de los videochats	No aplicable a los dispositivos BlackBerry OS	Esta regla especifica si en un dispositivo BlackBerry 10 se sincronizan los registros para la característica BBM Video con BlackBerry UEM.

De forma predeterminada, los archivos de registro de auditoría de la aplicación para dispositivos con BlackBerry 10 se guardan en *C:\Program Files\BlackBerry\UEM\Logs\<aaaammdd>* y los archivos de registro de auditoría de la aplicación para los dispositivos con BlackBerry OS se guardan en *C:\Program Files (x86)\Research in Motion \BlackBerry Enterprise Server\Logs\<aaaammdd>*.

Presentación de las acciones de dispositivo

Acciones que se han adoptado o están en curso en un dispositivo como resultado de los comandos que se envían desde la consola de gestión de BlackBerry UEM, tales como el bloqueo de un dispositivo, la desactivación del espacio de trabajo o la eliminación de los datos del dispositivo.

La disponibilidad de estos comandos depende del dispositivo y del tipo de activación.

El estado del comando de un dispositivo puede ser:

- Comando cancelado
- Comando completado por el dispositivo
- Comando enviado al dispositivo
- Envío de comando confirmado por el dispositivo
- Error de comando
- Comando en curso
- Notificación confirmada por el dispositivo
- Notificación enviada al dispositivo
- En cola

Ver acciones de dispositivo

1. En la barra de menú, haga clic en **Usuarios > Dispositivos gestionados**.
2. Busque una cuenta de usuario.
3. En los resultados de la búsqueda, haga clic en el nombre de una cuenta de usuario.
4. Haga clic en la pestaña del dispositivo del que desea ver las acciones del dispositivo.
5. Haga clic en **Ver acciones de dispositivo**.

Recuperación de registros del dispositivo

Puede recuperar los archivos de registro de los dispositivos a través de los métodos siguientes:

Método	Descripción	Dispositivos compatibles
Obtención de los registros de dispositivos con un comando de BlackBerry UEM	Puede recuperar los archivos de registro de los dispositivos mediante el comando "Obtener registros del dispositivo". Se realiza una instantánea de los archivos de registro para el dispositivo cada vez que utiliza el comando para recuperarlos. Se notifica a los usuarios la capacidad de recopilar archivos de registro del sistema durante la activación del dispositivo. Asimismo, podrán recibir una nueva notificación cuando envíe el comando para recuperar los archivos de registro en función de la configuración del dispositivo. Los dispositivos iOS y Android deben tener el BlackBerry UEM Client instalado y los archivos de registro recuperados deben ser únicamente registros BlackBerry UEM Client. Para los dispositivos BlackBerry 10, se recuperan todos los registros del dispositivo.	• iOS • Android • BlackBerry 10
Envío de archivos de registro desde BlackBerry UEM Client	Los usuarios de dispositivos pueden enviar por correo archivos de registro al administrador mediante el menú Ayuda de BlackBerry UEM Client.	• iOS • Android
Enviar archivos de registro del dispositivo BlackBerry 10 a BlackBerry Technical Support Services	Puede enviar archivos de registro del dispositivo con BlackBerry 10 a BlackBerry Technical Support Services mediante la regla de política de TI Enviar registros a BlackBerry para especificar si el dispositivo puede generar y enviar archivos de registro.	• BlackBerry 10
Envío de archivos de registro desde el catálogo de aplicaciones de BlackBerry UEM	Los usuarios de dispositivos con Windows 10 pueden enviar por correo archivos de registro al administrador mediante el menú Ayuda de BlackBerry UEM App Catalog.	• Windows 10

Obtención de los registros de dispositivos con un comando de BlackBerry UEM

Puede utilizar un comando de BlackBerry UEM para obtener los archivos de registro de los siguientes tipos de dispositivo:

- iOS
- Android
- BlackBerry 10

Antes de empezar:

- Los dispositivos con BlackBerry 10 deben disponer de BlackBerry 10 OS versión 10.3.1 o posterior. Para dispositivos activados con el tipo de activación "Trabajo y personal - Empresa ", los usuarios deben activar la recopilación remota. Para obtener más información, visite http://support.blackberry.com/kb y lea el artículo KB36424.
- Los dispositivos iOS y Android deben tener el BlackBerry UEM Client instalado.
- De forma predeterminada, la función Administrador secundario no puede recuperar archivos de registro.

1. En la barra de menú, haga clic en **Usuarios > Dispositivos gestionados**.
2. Busque una cuenta de usuario.
3. En los resultados de la búsqueda, haga clic en el nombre de la cuenta de usuario.
4. Haga clic en la pestaña del dispositivo.
5. En la ventana **Gestionar dispositivos**, haga clic en **Obtener registros del dispositivo**.
6. Haga clic en **Solicitud**.

Después de terminar:

Recupere los archivos de registro del dispositivo. De forma predeterminada, los archivos de registro se guardan en C:\Program Files\BlackBerry\UEM\Logs\device_logs.

Enviar archivos de registro del dispositivo BlackBerry 10 a BlackBerry Technical Support Services

Puede configurar el dispositivo BlackBerry 10 para permitirle enviar archivos de registro a BlackBerry Technical Support Services. Puede utilizar la regla de política de TI **Enviar registros a BlackBerry** para especificar si el dispositivo puede generar y enviar los archivos de registro.

El usuario debe tener una incidencia abierta con BlackBerry Technical Support Services y debe proporcionar el número de incidencia al enviar los archivos de registro del dispositivo. Si el usuario no proporciona un número de incidencia de soporte técnico o la dirección de correo correcta o el número PIN asociado a la incidencia de soporte técnico, el dispositivo mostrará un error al intentar enviar los archivos de registro del dispositivo.

Envío de archivos de registro desde BlackBerry UEM Client

Los usuarios pueden enviar archivos de registro desde BlackBerry UEM Client para los siguientes dispositivos:

- iOS
- Android
- Windows Phone 8

1. En el dispositivo, toque el icono **UEM Client**.
2. Toque **Ayuda**.
3. Toque **Enviar registros** o **Informe de errores**.
4. Seleccione la cuenta de correo en el dispositivo para enviar el archivo de registro.
5. Toque **Enviar**.
    - Los archivos de registro iOS y Android se adjuntarán al correo como un archivo .zip

- Los archivos de registro del dispositivo con Windows Phone 8 se incluirán en el cuerpo del correo electrónico.

Envío de archivos de registro desde el catálogo de aplicaciones de BlackBerry UEM

Para dispositivos con Windows 10, los usuarios pueden enviar archivos de registro desde BlackBerry UEM App Catalog.

1. En el dispositivo, toque el icono **Catálogo de aplicaciones**.
2. Toque **Ayuda**.
3. Toque **Informe de errores**.
4. Seleccione la cuenta de correo en el dispositivo para enviar el archivo de registro.
5. Toque **Enviar**. Los archivos de registro se adjuntan al correo como un archivo .zip.

Auditoría de eventos en BlackBerry UEM

BlackBerry UEM conserva los eventos de auditoría de seguridad y administrador en archivos de registro que puede utilizar para investigar cualquier acción de los administradores y las interacciones entre BlackBerry UEM los dispositivos.

BlackBerry UEM registra todas las acciones que realizan los administradores en la consola de administración y las muestra en la pantalla de auditoría. Puede filtrar la lista de acciones para que solo se muestren las acciones que son relevantes en su investigación. Para el análisis más detallado o para la generación de informes, puede exportar la lista filtrada a un archivo .csv.

Puede exportar eventos de auditoría de seguridad a un archivo .csv en la pantalla de configuración de auditoría. Los eventos de auditoría de seguridad incluyen las acciones del servidor como la entrega de los comandos o políticas, el inicio o la detención de una instancia de BlackBerry UEM, la iniciación o la rescisión de canales de confianza, el estado de validación del certificado y los cambios de la configuración de la auditoría. En la pantalla de configuración de auditoría, puede elegir los tipos de eventos de seguridad que desea registrar en el archivo de registro. Para algunos eventos, puede elegir si desea registrar el evento en función de si se completa correctamente o no se completa.

Nota:

Configuración de las opciones de auditoría

Puede activar o desactivar la auditoría de eventos de seguridad o administrador en BlackBerry UEM. Si la auditoría está activada, podrá elegir cuánto tiempo desea conservar los registros, el número de resultados que se mostrarán y cuándo eliminar los registros antiguos. Si la auditoría está desactivada, se borrarán todos los registros.

Nota: La activación de la auditoría de eventos de seguridad requiere numerosos recursos de base de datos. Puede descargar la calculadora de rendimiento y usarla para calcular los recursos necesarios.

1. En la barra de menú, haga clic en **Configuración** > **Infraestructura** > **Configuración de auditoría**.
2. En el panel derecho, haga clic en ✎.
3. En la sección**Configuración de auditoría de eventos de administrador**, lleve a cabo una de las siguientes acciones:

Tarea	Pasos
Active la auditoría de eventos de administrador	**a.** En el campo **Auditoría de eventos de administrador**, haga clic en **Activado**. **b.** En el campo **Retención de registro de auditoría de administrador**, escriba el número máximo de días que desea mantener un registro. **c.** En el campo **Número máximo de registros**, escriba el número máximo de registros que desea que se muestren en la interfaz de usuario. Si el número de registros supera este valor, el administrador debe acortar el intervalo de fechas o seleccionar una categoría para reducir el número de registros. **d.** En el campo **Hora de eliminación diaria (UTC)**, seleccione la hora en la que desea que se eliminen los registros.
Desactive la auditoría de eventos de administrador y depure todos los registros	**a.** En el campo **Auditoría de eventos de administrador**, haga clic en **Desactivado**.

4. En la sección**Configuración de auditoría de eventos de seguridad**, lleve a cabo una de las siguientes acciones:

Tarea	Pasos
Active la auditoría de eventos de seguridad	**a.** En el campo **Auditoría de eventos de seguridad**, haga clic en **Activado**. **b.** En el campo **Retención de registro de auditoría de seguridad**, escriba el número máximo de días que desea mantener un registro. **c.** En el campo **Hora de eliminación diaria (UTC)**, seleccione la hora en la que desea que se eliminen los registros antiguos. **d.** Para detener la auditoría de un evento de seguridad, haga clic en ✕ junto al tipo de evento. **e.** Para agregar eventos de seguridad para auditar, haga clic en +. Seleccione los eventos y haga clic en **Agregar**. **f.** Opcionalmente, si hay disponible una lista desplegable en la columna **Configuración** junto a un tipo de evento, seleccione la condición para registrar el evento.
Desactive la auditoría de eventos de seguridad y depure todos los registros	**a.** En el campo **Auditoría de eventos de seguridad**, haga clic en **Desactivado**.

5. Haga clic en **Guardar**.

Después de terminar:

- Reinicie el servicio de BlackBerry UEM Core en cada equipo que aloje una instancia de BlackBerry UEM.
- Vuelva a iniciar sesión en la consola de gestión.

Visualice y filtre los eventos de auditoría de administrador

La siguiente tarea es únicamente para ver y filtrar el registro de auditoría de eventos del administrador. Para ver el registro de eventos de auditoría de seguridad , consulte Exportación de eventos de auditoría de seguridad a un archivo .csv.

1. En la barra de menús, haga clic en **Auditoría y registro** > **Auditoría de sistema**.
2. Haga clic en **Editar**.
3. Seleccione una categoría y el intervalo de fechas. Haga clic en **Enviar**.
4. En **Filtros**, haga clic en una categoría para ampliarla.
5. Seleccione los filtros que desea aplicar y haga clic en **Enviar**.
6. Opcionalmente, en el panel de la derecha, haga clic en . Seleccione las columnas que desea ver.
7. Si fuera necesario, realice una de las siguientes acciones:
   - Para eliminar un filtro, haga clic en ✕ junto al filtro que desee eliminar.
   - Para borrar todos los filtros, haga clic en **Borrar todo**.

Después de terminar: Si es necesario, Exportación de eventos de auditoría de administrador a un archivo .csv.

Exportación de eventos de auditoría de administrador a un archivo .csv

Al exportar el archivo de eventos de auditoría de administrador a un archivo .csv, dicho archivo incluye los datos que filtró.

1. En la barra de menús, haga clic en **Auditoría y registro** > **Auditoría de sistema**.
2. Si fuera necesario, en el panel izquierdo, filtre el registro de auditoría para ver solo los datos que desea incluir en el archivo .csv.
3. Haga clic en y guarde el archivo.

Exportación de eventos de auditoría de seguridad a un archivo .csv

Al exportar el archivo de eventos de auditoría de seguridad a un archivo .csv, dicho archivo incluye todos los eventos de seguridad registrados.

1. En la barra de menú, haga clic en **Configuración** > **Infraestructura** > **Configuración de auditoría**.
2. En la sección **Configuración de auditoría eventos de seguridad**, haga clic en **Exportar** y guarde el archivo.

Eliminación de los registros de auditoría

Puede eliminar los registros de auditoría antes de la próxima eliminación diaria.

1. En la barra de menú, haga clic en **Configuración** > **Infraestructura** > **Configuración de auditoría**.
2. En la sección **Configuración de auditoría de eventos de administrador** o **Configuración de auditoría de eventos de seguridad**, haga clic en **Eliminar**.
3. Haga clic en **Eliminar**.

Crear notificaciones de eventos

Puede configurar las notificaciones de eventos para informar a los administradores por correo electrónico sobre determinados eventos de BlackBerry UEM. Algunos ejemplos de eventos:

- Se agrega una cuenta de usuario
- Uno de los dispositivos no cumple con los requisitos

- Un dispositivo está desactivado
- Una política de TI está asignada al grupo
- El certificado de APN caducará dentro de 30 días

Para obtener una lista completa de eventos, consulte Tipos de evento.

Cada notificación de eventos está asociado a una lista de distribución de correo electrónico, una programación y una plantilla de correo electrónico. Puede crear listas de distribución que incluyen direcciones de correo electrónico individuales, destinatarios con determinadas funciones de administrador o destinatarios que pertenecen a determinados grupos. Los programas definen los días de la semana y las veces que se envían las notificaciones. Las plantillas de correo electrónico definen el contenido de las notificaciones por correo electrónico.

Tareas relacionadas

Crear una plantilla de correo de notificación de evento

Crear una notificación de evento

Crear una notificación de evento para alertar a los administradores sobre los eventos de BlackBerry UEM.

Antes de empezar:

- Si no desea usar el correo electrónico de notificación de evento predeterminado, cree una plantilla de correo de notificación de evento.
- Crear una programación para una notificación de evento.
- Crear una lista de distribución para una notificación de evento.

1. En la barra de menú, haga clic en **Configuración > Configuración general**.
2. Haga clic en **Notificaciones de eventos**.
3. En la ficha **Notificaciones de eventos**, haga clic en +.
4. Seleccione un tipo de evento.
5. Haga clic en **Siguiente**.
6. En la lista desplegable **Fecha/hora para enviar la notificación por correo electrónico**, seleccione una de las opciones siguientes:
   - **Siempre tras un evento**: las notificaciones por correo electrónico se envían siempre que se produce un evento.
   - Un programa preconfigurado en la lista.
   - **Añadir nuevo programador**: cree un calendario y haga clic en **Guardar**.
7. En el campo **Destinatarios**, seleccione una de las opciones siguientes:
   - **Añadir nueva lista de distribución**: cree una lista de distribución y, a continuación, haga clic en **Guardar**.
   - Una lista de distribución preconfigurada.
8. En la lista desplegable **Plantilla de correo**, seleccione la plantilla de correo que desea utilizar para la notificación de evento.
9. En la lista desplegable **Estado**, seleccione **Activado** para activar la notificación de eventos o **Desactivado** para desactivarla.
10. Haga clic en **Vista previa del correo electrónico** para ver el correo electrónico de notificación de eventos y la lista de direcciones de correo electrónico para los destinatarios.
11. Haga clic en **Guardar**.

Crear una programación para una notificación de evento

Puede configurar previamente planes para asociarlos a las notificaciones de eventos. Las notificaciones de eventos se envían únicamente para los eventos que ocurren durante los días y horas definidos en el programa.

1. En la barra de menú, haga clic en **Configuración > Configuración general**.
2. Haga clic en **Notificaciones de eventos**.
3. En la ficha **Componentes de programación**, haga clic en +.
4. Escriba un nombre para la programación.
5. Seleccione los días de la semana a los que desee enviar notificaciones. Las notificaciones se envían únicamente para eventos que ocurren en los días seleccionados.
6. Seleccione una de las siguientes opciones:
   - Seleccione la casilla de verificación **Evento de todo el día**: las notificaciones se envían en cualquier momento.
   - Cancele la selección de la casilla de verificación **Evento de todo el día**: seleccione las horas del día en las que desea enviar las notificaciones. Las notificaciones se envían únicamente para eventos que ocurren en esas horas.
7. Haga clic en **Guardar**.

Crear una lista de distribución para una notificación de evento

Puede crear listas de distribución para asociarlas a las notificaciones de eventos. Las listas de distribución pueden incluir grupos de usuarios, funciones de administrador y direcciones de correo electrónico individuales.

1. En la barra de menú, haga clic en **Configuración > Configuración general**.
2. Haga clic en **Notificaciones de eventos**.
3. En la ficha **Lista de distribución**, haga clic en +.
4. Escriba un nombre para la lista de distribución.
5. Si desea incluir las direcciones de correo electrónico individuales, haga clic en + En la sección **destinatarios de correo electrónico**, escriba una dirección de correo electrónico y haga clic en **Guardar**.
6. Si desea incluir los administradores que pertenecen a un grupo, seleccione uno o más grupos en la lista **Grupos de usuarios** y haga clic ➔.
7. Si desea incluir los administradores que tienen una función particular, seleccione una o más funciones en la lista **Funciones de usuario disponibles** y haga clic ➔.
8. Haga clic en **Agregar**.

Desactivar una notificación de evento

Se puede desactivar una notificación de evento sin eliminar la notificación de eventos.

1. En la barra de menú, haga clic en **Configuración > Configuración general**.
2. Haga clic en **Notificaciones de eventos**.
3. En la columna **Tipo de notificación**, haga clic en una notificación de eventos.
4. En la lista desplegable **Estado** haga clic en **Apagado**.
5. Haga clic en **Guardar**.

Tipos de evento

Puede crear notificaciones de eventos para los siguientes tipos de eventos:

Administración de aplicaciones

- Aplicación agregada al grupo de usuarios
- Aplicación asignada al usuario
- Aplicación eliminada del grupo de usuarios
- Aplicación eliminada del usuario
- Definición de la aplicación creada
- Definición de la aplicación eliminada
- Definición de la aplicación actualizada
- Disposición del grupo de aplicaciones actualizada
- Disposición del grupo de usuarios actualizada

Firma de BDMI

- Error en la firma de BDMI

Conformidad

- Conformidad infringida
- Conformidad restaurada

Conectividad

- Error el enviar el correo de administrador
- Se ha restablecido la conexión con BlackBerry Infrastructure
- Error de conexión de BlackBerry Infrastructure
- Error al acceder a BlackBerry Gatekeeping Service

Dispositivo

- Dispositivo eliminado
- Cambio de propiedad del dispositivo
- Comando enviado
- Comando entregado
- Permitir BlackBerry Gatekeeping Service
- Cambio de SIM
- Estado del dispositivo del usuario cambiado

Inscripción

- Activación completada
- Desactivado

Grupo

- Grupo creado
- Grupo eliminado
- Grupo agregado al grupo de usuarios

- Grupo agregado al usuario
- Grupo eliminado del grupo de usuarios
- Usuario eliminado del grupo

Políticas y perfiles

- Política o perfil creado
- Política o perfil eliminado
- Política o perfil enviado
- Política o perfil entregado
- Política o perfil asignado a un grupo
- Política o perfil asignado a un usuario
- Política o perfil sin asignar al grupo
- Política o perfil sin asignar al usuario
- Almacenamiento de la firma de la política o el perfil
- Validación de la firma de la política o el perfil

Rendimiento

- Alerta de rendimiento del dispositivo

Usuario

- Usuario creado
- Usuario eliminado

Notificación automática de Apple

- Caducidad de certificado de APN (30 días antes de la caducidad)

Gestión de trabajos de BlackBerry Dynamics

BlackBerry UEM crea trabajos para procesar y completar las tareas complejas para aplicaciones de BlackBerry Dynamics. BlackBerry UEM mantiene una cola de trabajos y los procesa según el orden en el que se crearon. Una instancia de BlackBerry UEM debe completar el trabajo actual que está realizando antes de procesar el siguiente trabajo de la cola. Si el dominio incluye varias instancias de BlackBerry UEM, cualquier instancia que no está realizando un trabajo puede iniciar el siguiente trabajo en la cola.

Con la consola de gestión, puede ver los detalles de los trabajos que están en curso o completados (por ejemplo, el nombre de la instancia que ha procesado el trabajo, el tipo de trabajo, la hora de inicio y finalización, los errores que se han producido, etc.). También puede eliminar manualmente los registros de trabajos desde la consola de gestión.

Si desea que BlackBerry UEM elimine automáticamente registros de trabajos después de un número específico de días, puede configurar las propiedades de BlackBerry UEM. Para obtener más información, consulte el contenido referente a Configuración.

1. En la consola de gestión, en la barra de menú, haga clic en **Configuración > BlackBerry Dynamics**.
2. Haga clic en **Trabajos**.
3. Lleve a cabo cualquiera de las tareas siguientes:

Tarea	Pasos
Vea los detalles de un trabajo.	Haga clic en un trabajo.
Elimine los registros de auditoría.	No puede recuperar un registro de trabajo después de eliminarlo. Eliminar el registro de trabajo que está en curso no evita que el trabajo se lleve a cabo correctamente. **a.** Seleccione uno o más trabajos. **b.** Haga clic en 🗑. **c.** Haga clic en **Aceptar**.
Elimine todos los registros de trabajos que sean anteriores a un determinado número de días.	**Nota:** La siguiente tarea elimina todos los registros de trabajos anteriores al número especificado de días, incluso aquellos que no se pueden ver en la pantalla Trabajos (por ejemplo, trabajos de sincronización de Active Directory). **a.** En la lista desplegable **Eliminar trabajos después de**, haga clic en el número de días correspondiente. **b.** Haga clic en **Eliminar**.

Uso de SNMP para controlar BlackBerry UEM

Puede utilizar herramientas SNMP de terceros para controlar la actividad de BlackBerry UEM.

Para obtener más información sobre la configuración SNMP para controlar BlackBerry UEM Core,BlackBerry Secure Connect Plus,BlackBerry Secure Gateway y otros componentes de BlackBerry UEM, consulte el contenido referente a Configuración.

Para obtener más información sobre los principales contadores SNMP para controlar el rendimiento y la actividad, consulte el contenido HTML.

Uso de los informes de panel

El panel utiliza gráficos para presentar la información de los servicios de BlackBerry UEM acerca de los usuarios y los dispositivos en el sistema. Puede utilizar el cursor para desplazarse sobre un punto de datos (por ejemplo, un sector de un gráfico circular) para ver información acerca de los usuarios o los dispositivos.

Si necesita más información, puede mostrar un informe del gráfico para consultar información detallada acerca de los usuarios o dispositivos. El número máximo de registros en un informe es de 2000. Puede generar un archivo .csv a partir de un informe y exportar el archivo para próximos análisis o fines de notificaciones de errores.

Para abrir y administrar una cuenta de usuario, puede hacer clic en el usuario o en el dispositivo en un informe. Cuando haya terminado con una cuenta, puede hacer clic en Atrás en la página (no en el navegador) para volver al informe.

En la siguiente tabla se describe la información que muestra cada informe de panel.

Informe de panel	Descripción
Dispositivos con y sin roaming	Una lista de usuarios con los dispositivos que se encuentran actualmente en un estado de roaming
Activaciones del dispositivo	Una representación dinámica de los dispositivos activados cada mes en la empresa a lo largo de un periodo de 12 meses, que se basa en cuándo los dispositivos se activaron inicialmente. Los números cambian para reflejar los dispositivos activados actualmente. Por ejemplo, si un dispositivo que se activó en agosto está desactivado, el número de dispositivos que se muestran en agosto se reduce en uno.
Las principales 5 aplicaciones asignadas instaladas	Las cinco aplicaciones más comunes asignadas por la empresa e instaladas en los dispositivos
Dispositivos por plataforma	Un desglose del número de dispositivos de la empresa por plataforma
Conformidad de los dispositivos	Una lista de los problemas detectados en los dispositivos BlackBerry 10, iOS, Android y Windows Phone de la empresa
Dispositivos por última hora de contacto	El número de días que han transcurrido desde que los dispositivos contactaron por última vez con el servidor
Dispositivos por operadores	Un desglose del número de dispositivos de la empresa por proveedor de servicios
Los principales 5 modelos de dispositivo	Los cinco modelos de dispositivos móviles más comunes en la empresa

Cambio del tipo de gráfico

Puede cambiar el tipo de gráfico utilizado para representar gráficamente la información.

Haga clic en ⚙ junto a un gráfico y seleccione un tipo de gráfico de la lista desplegable.

Exportación de un informe de panel a un archivo .csv

1. Para abrir un informe, haga clic en un gráfico.
2. Para ordenar los registros basados en la columna seleccionada, haga clic en el encabezado de una columna.
3. Haga clic en **Exportar** y guarde el archivo.

Visualización de actividad de llamadas telefónicas y SMS/MMS para dispositivos Android con un perfil de trabajo y dispositivos Samsung KNOX Workspace

Puede ver la actividad de llamadas telefónicas y SMS/MMS para dispositivos Android con un perfil de trabajo y dispositivos. Samsung KNOX Workspace BlackBerry UEM registra esta actividad para dispositivos que están activados con "Solo espacio de trabajo (Premium)", "Trabajo y personal: control total (Samsung KNOX)" y "Solo

espacio de trabajo (Samsung KNOX)". No se registra ninguna actividad de llamadas telefónicas y SMS/MMS si los dispositivos se activan con perfiles distintos a los indicados.

BlackBerry UEM genera archivos de registro .CSV separados tanto para llamadas telefónicas como para SMS/MMS. De forma predeterminada, estos archivos de registro se guardan en `<unidad>:\Program Files\BlackBerry\UEM\Logs\<fecha o nombre de carpeta>` BlackBerry UEM pone nombre a los archivos de registro *<nombre del servidor>_<identificador del componente>_<versión de definición de evento>_<aaaammdd>_<número de registro>.<extensión de archivo>* (por ejemplo, BBServer01_phone_1.0_20160730_0001.csv). Consulte Uso de archivos de registro para obtener información sobre cómo buscar y leer los archivos de registro.

Ver y guardar un informe de dispositivo

Puede generar un informe de dispositivo para ver información detallada acerca de cada dispositivo asociado a BlackBerry UEM.

1. En la barra de menú, haga clic en **Usuarios > Dispositivos gestionados**.
2. Busque una cuenta de usuario.
3. En los resultados de la búsqueda, haga clic en el nombre de la cuenta de usuario.
4. Seleccione la pestaña dispositivo.
5. Haga clic en **Ver informe del dispositivo**.
6. Haga clic en **Exportar** para guardar el informe de dispositivo en un archivo en el equipo si es necesario.

Exportación de informes de implementación de aplicaciones

Puede exportar informes de implementación de aplicaciones a un archivo .html desde la pantalla de aplicaciones en la consola de gestión. El informe incluye información acerca de las aplicaciones implementadas por BlackBerry UEM y los usuarios que tienen instaladas actualmente las aplicaciones en sus dispositivos. Por ejemplo, puede encontrar información del dispositivo de todos los usuarios que tienen una aplicación específica, incluido el ID del dispositivo, el modelo y la versión del sistema operativo.

Puede elegir las aplicaciones que desea incluir en un informe. Cada aplicación que elija para incluir en el informe se encontrará en una sección independiente que indicará la información de la versión de la aplicación y la información del dispositivo para cada usuario que tenga la aplicación instalada.

Nota: Para los dispositivos iOS con el tipo de activación Privacidad del usuario, el informe indica todos los dispositivos que tienen la aplicación instalada. BlackBerry UEM no puede confirmar si la aplicación sigue instalada en el dispositivo cuando se genere el informe.

También puede abrir el archivo .html mediante Microsoft Excel para un análisis más detallado.

Exportación de un informe de implementación de aplicaciones a un archivo .html

1. En la barra de menú, haga clic en **Aplicaciones > Aplicaciones**.
2. Para cada aplicación que desee incluir en el informe, seleccione la casilla de verificación situada junto a la aplicación. Puede seleccionar la casilla de verificación en la parte superior de la lista aplicaciones para seleccionar todas las aplicaciones.
3. Haga clic en y guarde el archivo.

Informes de infracción de conformidad y actividad de aplicaciones de BlackBerry Dynamics

Cuando se integra BlackBerry UEM y BlackBerry Dynamics, puede exportar datos sobre infracción de conformidad o actividad de la aplicación de BlackBerry Dynamics desde la consola de gestión. Puede utilizar esta información para tomar medidas con respecto a cualquier actividad sospechosa o inadecuada. Los informes de actividad de la aplicación incluyen datos de actividad de cada aplicación de BlackBerry Dynamics (por ejemplo, información de versión de la aplicación, fecha de activación y el último contacto con el servidor). Los informes de infracción de conformidad incluyen datos sobre infracción de conformidad de cada aplicación (por ejemplo, las reglas de la política que se han infringido y el momento en el que se ha producido la infracción).

Exportación de informes de aplicaciones de BlackBerry Dynamics a un archivo .csv

Cada informe tiene un límite de 5000 registros.

1. En la barra de menú, haga clic en **Configuración > BlackBerry Dynamics > Informes**.
2. En la sección **Exportar datos a .csv**, seleccione el tipo de informe que desea exportar:
   - **Actividad de aplicaciones de BlackBerry Dynamics**
   - **Infracciones de cumplimiento de la aplicación BlackBerry Dynamics**
3. Haga clic en **Exportar** y guarde el archivo.

Control del rendimiento de la aplicación BlackBerry Work

Puede controlar el rendimiento de la aplicación BlackBerry Work y seleccionar los problemas sobre los que desea informar.

Activar control de BlackBerry Work

Para habilitar el control de BlackBerry Work, debe ajustar la configuración de la aplicación que se le asigna.

1. En la barra de menú, haga clic en **Aplicaciones**.
2. Haga clic en la aplicación de BlackBerry Work que desea controlar.
3. En la pestaña BlackBerry Dynamics, en la tabla de configuración de la aplicación, haga clic en el nombre de la configuración de la aplicación que desea editar.
4. En la pestaña **Informes de rendimiento**, configure una de las siguientes opciones:
   - **Habilitar informes de rendimiento**: especifique si desea controlar el rendimiento de la aplicación BlackBerry Work.
   - **Error de conexión HTTP**: especifique si desea informar de los errores de conexión HTTP entre BlackBerry Work y los servidores de aplicaciones especificados.
   - **Tiempo de respuesta HTTP**: especifique si desea informar de las respuestas HTTP que tardan más del tiempo especificado. Introduzca las direcciones de servidor de aplicaciones que desea controlar.
   - **Código de estado HTTP**: especifique si desea informar de un código de estado HTTP especificado. Introduzca las direcciones de servidor de aplicaciones que desea controlar.
   - **No enviar informes de duración (en segundos)**: especifique la cantidad de tiempo que se debe esperar antes de enviar otro informe.
5. Haga clic en **Guardar**.

Ver notificaciones de alerta de rendimiento del dispositivo

Antes de empezar:

- Activar control de BlackBerry Work

1. En la barra de menús, haga clic en **Auditoría y registro** > **Rendimiento del dispositivo**.
2. Seleccione una categoría y el intervalo de fechas. Haga clic en **Submit**.
3. En **Filtros**, haga clic en una categoría para ampliarla.
4. Seleccione los filtros que desea aplicar y haga clic en **Enviar**.
5. Si fuera necesario, realice una de las siguientes acciones:
   - Para eliminar un filtro, haga clic en ✕ junto al filtro que desee eliminar.
   - Para borrar todos los filtros, haga clic en **Borrar todo**.
6. Para exportar los resultados a un archivo .csv, haga clic en .

Ver una alerta de rendimiento para un único dispositivo

En lugar de ver una lista de alertas de rendimiento basadas en la fecha y el tipo de alerta, también puede ver todas las alertas de rendimiento de un solo dispositivo en las últimas 24 horas. Si hay alertas de rendimiento para un dispositivo, aparecerá un icono de precaución en la ficha del dispositivo y un mensaje que le indicará cuántas alertas se han detectado en el dispositivo.

Antes de empezar:

- Activar control de BlackBerry Work

1. En la barra de menú, haga clic en **Usuarios > Dispositivos gestionados**.
2. Busque una cuenta de usuario.
3. En los resultados de la búsqueda, haga clic en el nombre de la cuenta de usuario.
4. Seleccione la pestaña del dispositivo del que desea ver las alertas. Un dispositivo con alertas de rendimiento o infracciones de la conformidad se marcará con un icono de precaución.
5. Si hay alertas de rendimiento para el dispositivo, haga clic en **Ver todo** junto al mensaje de alerta de rendimiento para ver la lista de alertas de rendimiento para ese dispositivo.

Configuraciones de perfil

En esta sección se ofrecen descripciones detalladas de las opciones de los perfiles que tienen un gran número de configuraciones para ayudarle a configurar el correo electrónico, las conexiones de red y otras funciones.

Para los perfiles con un pequeño número de configuraciones, consulte el tema sobre la creación del perfil para ver descripciones de las configuraciones.

Configuración del perfil de correo

Puede utilizar una variable en cualquier ajuste de perfil que sea un campo de texto para hacer referencia a un valor en lugar de especificar el valor real. BlackBerry UEM admite variables predeterminadas que son variables predefinidas y personalizadas que se definen. Los perfiles de correo son compatibles con los siguientes tipos de dispositivos:

- BlackBerry 10
- iOS
- macOS
- Android
- Windows

En algunos casos, la versión mínima del SO del dispositivo requerida para que sea compatible con una configuración es una versión no admitida por BlackBerry UEM. Para obtener más información acerca de las versiones compatibles, consulte la Matriz de compatibilidad.

Común: ajustes del perfil de correo

Común: ajuste del perfil de correo	Descripción
Nombre de dominio	Este ajuste especifica el nombre del dominio del servidor de correo.
Dirección de correo	En la configuración se especifica la dirección de correo del usuario. Si el perfil es para varios usuarios, puede utilizar la variable %UserEmailAddress%.
Nombre de host o dirección IP	En la configuración se especifica el nombre de host o la dirección IP del servidor de correo.
Nombre de usuario	En la configuración se especifica el nombre de usuario del usuario. Si el perfil es para varios usuarios, puede utilizar la variable %UserName%.
Servidores de enlace automáticos	Si ha configurado grupos de servidores para dirigir el tráfico de BlackBerry Secure Gateway o el tráfico de BlackBerry Gatekeeping Service hacia una conexión regional específica en la BlackBerry Infrastructure, esta opción especifica el grupo de servidores adecuado. Para obtener más información acerca de BlackBerry Connectivity Node y los grupos de servidores, consulte el contenido de Planificación y el contenido de Instalación y actualización.

BlackBerry 10: ajustes del perfil de correo

BlackBerry 10: ajuste del perfil de correo	Descripción
Nombre de cuenta	En la configuración se especifica el nombre de la cuenta de correo de trabajo que aparece en BlackBerry Hub y en los ajustes del dispositivo. Puede utilizar una variable como, por ejemplo, %UserEmailAddress%.
Puerto	En la configuración se especifica el puerto que se utiliza para conectarse al servidor de correo.
Configuración de entrega	
Tipo de perfil	En la configuración se especifica si desea que este perfil sea compatible con Exchange ActiveSync o IBM Notes Traveler. Valores posibles: • Exchange ActiveSync • IBM Notes Traveler El valor predeterminado es "Exchange ActiveSync".
Servidor SyncML	En la configuración se especifica el FQDN del servidor IBM Notes Traveler que un dispositivo BlackBerry 10 puede utilizar para sincronizar los datos de tareas pendientes. Esta configuración es válida únicamente si la opción "Tipo de perfil" se establece en "IBM Notes Traveler".
Puerto de SyncML	En la configuración se especifica el puerto del servidor Notes Traveler que un dispositivo BlackBerry 10 puede utilizar para sincronizar los datos de tareas pendientes. Esta configuración es válida únicamente si la opción "Tipo de perfil" se establece en "IBM Notes Traveler".
Utilice SSL para SyncML	En la configuración se especifica si un dispositivo BlackBerry 10 necesita realizar una conexión SSL en el servidor Notes Traveler. Esta configuración es válida únicamente si la opción "Tipo de perfil" se establece en "IBM Notes Traveler".
Push activo	En la configuración se especifica si el servidor de correo puede insertar mensajes de correo en un dispositivo BlackBerry 10.

BlackBerry 10: ajuste del perfil de correo	Descripción
Intervalo entre sincronizaciones	En la configuración se especifica la frecuencia con la que un dispositivo BlackBerry 10 comprueba el servidor de correo para buscar nuevos mensajes. Esta configuración es válida únicamente si se no ha seleccionado la opción "Push activo". Valores posibles: • Manual • 5 minutos • 15 minutos • 30 minutos • 1 hora • 2 horas • 4 horas • 24 horas El valor predeterminado es "15 minutos".
Días para sincronizar	En la configuración se especifica el número de días transcurridos para sincronizar los mensajes de correo y los datos del organizador en un dispositivo BlackBerry 10. Valores posibles: • 1 día • 3 días • 7 días • 14 días • 1 mes • Indefinidamente El valor predeterminado es "1 mes".
Requiere sincronización manual cuando se encuentra en itinerancia	En la configuración se especifica si un usuario debe iniciar la sincronización entre un dispositivo BlackBerry 10 y el servidor de correo cuando el usuario tiene activado el roaming.
Utilizar SSL	En la configuración se especifica si un dispositivo debe utilizar SSL para conectarse al servidor de correo.
Sincronización del calendario	En la configuración se especifica si desea que un dispositivo BlackBerry 10 sincronice las entradas de calendario con el servidor de correo.
Sincronización de los contactos	En la configuración se especifica si desea que un dispositivo BlackBerry 10 sincronice los contactos con el servidor de correo.
Sincronización del correo	En la configuración se especifica si desea que un dispositivo BlackBerry 10 sincronice los mensajes de correo con el servidor de correo.

BlackBerry 10: ajuste del perfil de correo	Descripción
Sincronización de la memoria	En la configuración se especifica si desea que un dispositivo BlackBerry 10 sincronice los datos de memoria con el servidor de correo. Esta configuración es válida únicamente si la opción "Tipo de perfil" se establece en "Exchange ActiveSync".
Sincronización de tareas	En la configuración se especifica si desea que un dispositivo BlackBerry 10 sincronice los datos de tareas con el servidor de correo. Esta configuración es válida únicamente si la opción "Tipo de perfil" se establece en "Exchange ActiveSync".
Sincronización pendiente	En la configuración se especifica si desea que un dispositivo BlackBerry 10 sincronice los datos de tareas pendientes mediante Notes Traveler. Esta configuración es válida únicamente si la opción "Tipo de perfil" se establece en "IBM Notes Traveler".
Configuración de correo electrónico seguro	
Sugiera la codificación predeterminada para los mensajes de salida	En la configuración se especifica si un dispositivo BlackBerry 10 sugiere la codificación predeterminada, (por ejemplo, texto sin formato, firmar, cifrar o firmar y cifrar) para todos los mensajes de correo salientes. Si la configuración se establece en "Permitir", un usuario puede elegir si el dispositivo sugiere la codificación predeterminada o sugiere la codificación basada en el historial de mensajes. Si la configuración se establece en "Obligatorio", el dispositivo sugiere la codificación predeterminada. Si la configuración se establece en "No permitir", el dispositivo sugiere la codificación basada en el historial de mensajes. Valores posibles: • Permitir • Obligatorio • No permitir El valor predeterminado es "Permitir". El requisito mínimo es BlackBerry 10 OS versión 10.3.1.
Configuración S/MIME	

BlackBerry 10: ajuste del perfil de correo	Descripción
Compatibilidad de S/MIME	En la configuración se especifica si desea que las extensiones S/MIME estén activadas en el dispositivo BlackBerry 10. Si la configuración se establece en "Permitir", un usuario puede elegir si desea activar o no la protección S/MIME en el dispositivo. Si la configuración se establece en "Obligatorio", la protección S/MIME se activa en el dispositivo y el usuario no puede desactivarla. Si la configuración se establece en "No permitir", la protección S/MIME se desactiva en el dispositivo y el usuario no puede activarla. Para enviar mensajes de correo cifrados, un usuario debe tener la clave pública del destinatario en el dispositivo o en una tarjeta inteligente. Para enviar mensajes de correo con firma digital, la clave privada del usuario debe estar en el dispositivo o en una tarjeta inteligente. Dicha configuración tiene prioridad sobre la configuración "Mensajes de S/MIME con firma digital" y la configuración "Mensajes de S/MIME cifrados". La configuración afecta a la configuración "Compatibilidad de PGP". Si el ajuste se establece en "Obligatorio", el ajuste "Compatibilidad de PGP" se debe establecer en "No permitir". Valores posibles: • Permitir • Obligatorio • No permitir El valor predeterminado es "Permitir".
Mensajes de S/MIME con firma digital	En la configuración se especifica si desea que un dispositivo BlackBerry 10 envíe mensajes de correo de salida con una firma digital. Si la configuración se establece en "Permitir", un usuario puede elegir si desea firmar los mensajes de correo salientes de forma digital. Si la configuración se establece en "Obligatorio", un usuario debe firmar los mensajes de correo salientes de forma digital. Si la configuración se establece en "No permitir", un usuario no puede firmar los mensajes de correo salientes de forma digital Para enviar mensajes de correo con firma digital, la clave privada del usuario debe estar en el dispositivo o en una tarjeta inteligente. Este ajuste es válido únicamente si el ajuste "compatibilidad de S/MIME" se establece en "Permitir" o "Requerido". Si la configuración "compatibilidad de S/MIME" se establece en "Obligatorio" y tanto esta configuración como la configuración de "Mensajes de S/MIME cifrados" se establecen en "No permitir", la configuración de "Mensajes de S/MIME cifrados" y esta configuración se ignoran y se utiliza la configuración predeterminada "Permitir" para ambas configuraciones. Valores posibles: • Permitir • Obligatorio • No permitir El valor predeterminado es "Permitir".

BlackBerry 10: ajuste del perfil de correo	Descripción
Mensajes de S/MIME cifrados	En la configuración se especifica si desea que un dispositivo BlackBerry 10 cifre los mensajes de correo de salida con el cifrado S/MIME. Si la configuración se establece en "Permitir", un usuario puede elegir o no si desea cifrar los mensajes de correo salientes. Si la configuración se establece en "Obligatorio", un usuario debe cifrar los mensajes de correo salientes. Si la configuración se establece en "No permitir", un usuario no puede cifrar los mensajes de correo salientes. Para enviar mensajes de correo cifrados, un usuario debe tener la clave pública del destinatario en el dispositivo o en una tarjeta inteligente. Este ajuste es válido únicamente si el ajuste "compatibilidad de S/MIME" se establece en "Permitir" o "Requerido". Si la configuración "Compatibilidad de S/MIME" se establece en "Obligatorio" y tanto esta configuración como la configuración de "Mensajes de S/MIME con firma digital" se establecen en "No permitir", la configuración de "Mensajes de S/MIME con firma digital" y esta configuración se ignoran y la configuración predeterminada de "Permitir" se utiliza para ambas configuraciones. Valores posibles: • Permitir • Obligatorio • No permitir El valor predeterminado es "Permitir".
Algoritmos de cifrado	En la configuración se especifican los algoritmos de cifrado que un dispositivo BlackBerry 10 puede utilizar para cifrar mensajes de correo electrónico protegidos con S/MIME. Valores posibles: • AES (256 bits) • AES (192 bits) • AES (128 bits) • Triple DES • RC2 El valor predeterminado es un valor nulo.
Configuración de PGP	

BlackBerry 10: ajuste del perfil de correo	Descripción
Compatibilidad de PGP	En la configuración se especifica si desea que la protección PGP esté activada en el dispositivo BlackBerry 10. Si la configuración se establece en "Permitir", un usuario puede elegir si desea activar o no la protección PGP en el dispositivo. Si la configuración se establece en "Obligatorio", la protección PGP se activa en el dispositivo y el usuario no puede desactivarla. Si la configuración se establece en "No permitir", la protección PGP se desactiva en el dispositivo y el usuario no puede activarla. Para enviar mensajes de correo cifrados, un usuario debe tener la clave pública del destinatario en el dispositivo. Para enviar mensajes de correo con firma digital, la clave privada del usuario debe estar en el dispositivo. La configuración "Compatibilidad de S/MIME" afecta a esta configuración. Si la "Compatibilidad de S/MIME" se establece en "Obligatorio" o si la "Compatibilidad de S/MIME" se establece en "Permitir" y la configuración de "Mensajes de S/MIME con firma digital" o de "Mensajes de S/MIME cifrados" se establece en "Obligatorio", esta configuración se debe establecer en "No permitir". Valores posibles: • Permitir • Obligatorio • No permitir El valor predeterminado es "Permitir". El requisito mínimo es BlackBerry 10 OS versión 10.3.1.
Dirección de Symantec Encryption Management Server	En la configuración se especifica la dirección FQDN o IP del servidor Symantec Encryption Management Server de la empresa para solicitar que un usuario de dispositivo BlackBerry 10 inscriba el dispositivo en dicho servidor para enviar mensajes PGP. La configuración "Compatibilidad de PGP" afecta a esta configuración. El dispositivo utiliza esta configuración si la configuración "Compatibilidad de PGP" se establece en "Permitir" o en "Obligatorio". El requisito mínimo es BlackBerry 10 OS versión 10.3.1.

BlackBerry 10: ajuste del perfil de correo	Descripción
Método de inscripción del servidor Symantec Encryption Management Server	En la configuración se especifica el método que un usuario de dispositivo BlackBerry 10 debe utilizar para inscribir el dispositivo en el servidor Symantec Encryption Management Server de la empresa. Si la configuración se establece en "Autenticación de correo", el dispositivo solicita al usuario que introduzca su dirección de correo. Si la configuración se establece en "Autenticación de Microsoft Active Directory", el dispositivo solicita al usuario que introduzca el dominio nombre de usuario y la contraseña. La configuración "Compatibilidad de PGP" afecta a esta configuración. El dispositivo utiliza esta configuración si la configuración "Compatibilidad de PGP" se establece en "Permitir" o en "Obligatorio". Valores posibles: • Autenticación de correo • Autenticación de Microsoft Active Directory El valor predeterminado es "Autenticación de correo". El requisito mínimo es BlackBerry 10 OS versión 10.3.1.
Perfiles asociados	
Tipo de autenticación	En la configuración se especifica el tipo de autenticación que un dispositivo BlackBerry 10 debe utilizar para conectarse al servidor de correo. Valores posibles: • Ninguno • SCEP • Credencial de usuario El valor predeterminado es "Ninguno".
Perfil SCEP asociado	En la configuración se especifica el perfil SCEP asociado que un dispositivo BlackBerry 10 debe utilizar para inscribir un certificado de cliente con el objetivo de autenticarlo con el servidor de correo. Esta configuración es válida únicamente si la opción "Tipo de autenticación" se establece en "SCEP".
Perfil de credenciales de usuario asociado	En la configuración se especifica el perfil de credenciales de usuario asociado que un dispositivo BlackBerry 10 debe utilizar para obtener un certificado de cliente con el objetivo de autenticarlo con el servidor de correo. Esta configuración es válida únicamente si la opción "Tipo de autenticación" se establece en "Credenciales del usuario". El requisito mínimo es BlackBerry 10 OS versión 10.3.1.
Clasificación de los mensajes	

BlackBerry 10: ajuste del perfil de correo	Descripción
Archivo de clasificación de mensajes (.json)	En la configuración se especifica el archivo de clasificación de mensajes para enviar a los dispositivos de los usuarios. El requisito mínimo es BlackBerry 10 OS versión 10.3.1.

Conceptos relacionados

Aplicación de un correo protegido mediante la clasificación de mensajes

Perfil de S/MIME y dependencias de configuración de dispositivo

La siguiente tabla muestra las dependencias entre la configuración S/MIME que se puede establecer en BlackBerry UEM y la configuración S/MIME que los usuarios pueden establecer en los dispositivos BlackBerry 10. Dependiendo de lo que se han establecido, las opciones en la lista desplegable Codificación de los dispositivos cambian. Los dispositivos ignoran el valor para algunos ajustes si una configuración con más prioridad (por ejemplo, "Compatibilidad de S/MIME") entra en conflicto con el valor de esa configuración.

Configuración de compatibilidad de S/MIME	Configuración de mensajes de S/MIME con firma digital	Configuración de mensajes de S/MIME cifrados	Configuración S/MIME en el dispositivo	Lista desplegable de codificación en dispositivo
Permitido	Permitido	Permitido	El usuario puede activar o desactivar la protección S/MIME.	• Texto sin formato • Firmar (S/MIME) • Cifrar (S/MIME) • Firmar y cifrar (S/MIME)
	Permitido	Obligatorio	La protección S/MIME está activada. El usuario no puede desactivarla.	• Cifrar (S/MIME) • Firmar y cifrar (S/MIME)
	Permitido	No permitido	El usuario puede activar o desactivar la protección S/MIME.	• Texto sin formato • Firmar (S/MIME)
	Obligatorio	Permitido	La protección S/MIME está activada. El usuario no puede desactivarla.	• Firmar (S/MIME) • Firmar y cifrar (S/MIME)
	Obligatorio	Obligatorio	La protección S/MIME está activada. El usuario no puede desactivarla.	Firmar y cifrar (S/MIME)
	Obligatorio	No permitido	La protección S/MIME está activada. El usuario no puede desactivarla.	Firmar (S/MIME)

Configuración de compatibilidad de S/MIME	Configuración de mensajes de S/MIME con firma digital	Configuración de mensajes de S/MIME cifrados	Configuración S/MIME en el dispositivo	Lista desplegable de codificación en dispositivo
	No permitido	Permitido	El usuario puede activar o desactivar la protección S/MIME.	• Texto sin formato • Cifrar (S/MIME)
	No permitido	Obligatorio	La protección S/MIME está activada. El usuario no puede desactivarla.	Cifrar (S/MIME)
	No permitido	No permitido	El usuario puede activar o desactivar la protección S/MIME, pero no puede cifrar o firmar mensajes porque los perfiles necesarios están establecidos en No permitido.	Texto sin formato
Obligatorio	Permitido	Permitido	La protección S/MIME está activada. El usuario no puede desactivarla.	• Firmar (S/MIME) • Cifrar (S/MIME) • Firmar y cifrar (S/MIME)
	Permitido	Obligatorio	La protección S/MIME está activada. El usuario no puede desactivarla.	• Cifrar (S/MIME) • Firmar y cifrar (S/MIME)
	Permitido	No permitido	La protección S/MIME está activada. El usuario no puede desactivarla.	Firmar (S/MIME)
	Obligatorio	Permitido	La protección S/MIME está activada. El usuario no puede desactivarla.	• Firmar (S/MIME) • Firmar y cifrar (S/MIME)
	Obligatorio	Obligatorio	La protección S/MIME está activada. El usuario no puede desactivarla.	Firmar y cifrar (S/MIME)
	Obligatorio	No permitido	La protección S/MIME está activada. El usuario no puede desactivarla.	Firmar (S/MIME)
	No permitido	Permitido	La protección S/MIME está activada. El usuario no puede desactivarla.	Cifrar (S/MIME)

Configuración de compatibilidad de S/MIME	Configuración de mensajes de S/MIME con firma digital	Configuración de mensajes de S/MIME cifrados	Configuración S/MIME en el dispositivo	Lista desplegable de codificación en dispositivo
	No permitido	Obligatorio	La protección S/MIME está activada. El usuario no puede desactivarla.	Cifrar (S/MIME)
	No permitido (La configuración se ignora)	No permitido (La configuración se ignora)	La protección S/MIME está activada. El usuario no puede desactivarla.	• Firmar (S/MIME) • Cifrar (S/MIME) • Firmar y cifrar (S/MIME)
No permitido	Se ignora cualquier configuración	Se ignora cualquier configuración	La protección S/MIME está desactivada. El usuario no puede activarla.	Texto sin formato

Perfil de PGP y dependencias de configuración de dispositivo

La siguiente tabla muestra las dependencias entre el ajuste "Compatibilidad de PGP" que se puede configurar en BlackBerry UEM y los ajustes PGP que los usuarios pueden configurar en los dispositivos BlackBerry 10. Dependiendo de lo que se establezca en el ajuste "Compatibilidad de PGP", las opciones en la lista desplegable Codificación de los dispositivos cambian. Los dispositivos ignoran el valor de esta configuración si una con más prioridad (por ejemplo, "Compatibilidad de S/MIME") entra en conflicto con el valor de dicha configuración.

Configuración de compatibilidad de PGP	Ajustes de PGP en el dispositivo	Lista desplegable de codificación en dispositivo
Permitir	Los usuarios pueden activar o desactivar la protección PGP.	• Texto sin formato • Firmar (PGP) • Cifrar (PGP) • Firmar y cifrar (PGP)
Obligatorio	La protección PGP está activada. El usuario no puede desactivarla.	• Firmar (PGP) • Cifrar (PGP) • Firmar y cifrar (PGP)
No permitir	La protección PGP está desactivada. El usuario no puede activarla.	Sin lista desplegable. Se utiliza texto sin formato.

iOS: ajustes del perfil de correo

iOS: ajuste del perfil de correo	Descripción
Configuración de entrega	

iOS: ajuste del perfil de correo	Descripción
Permitir que los mensajes se muevan	En la configuración se especifica si desea que los usuarios puedan mover mensajes de correo desde esta cuenta a otra cuenta de correo en el dispositivo iOS.
Permitir la sincronización de direcciones recientes	En la configuración se especifica si un usuario del dispositivo iOS puede sincronizar direcciones utilizadas recientemente a través de los dispositivos.
Utilizar solo con correo	En la configuración se especifica si desea que las aplicaciones que no sean la aplicación de correo en el dispositivo iOS puedan utilizar esta cuenta para enviar mensajes de correo.
Activar S/MIME	En la configuración se especifica si un usuario del dispositivo iOS puede enviar mensajes de correo protegidos con S/MIME.
Activar mensajes de S/MIME con firma digital	En la configuración se especifica si desea que un dispositivo envíe mensajes de salida con una firma digital. Esta configuración se aplica únicamente a dispositivos con iOS 10.3 o versiones posteriores.
Credenciales de firma	En la configuración se especifica cómo los dispositivos encuentran los certificados necesarios para firmar los mensajes. Esta configuración es válida únicamente si se ha seleccionado la opción "Activar S/MIME". Valores posibles: • Certificado compartido • SCEP • Credencial de usuario Después de elegir el tipo de perfil que desea utilizar, puede especificar el certificado compartido, el SCEP o el perfil de credenciales de usuario.
Certificado compartido de firma	En la configuración se especifica el perfil de certificado compartido para un certificado de cliente que el dispositivo iOS utiliza para firmar mensajes de correo. Esta configuración es válida únicamente si se ha seleccionado la opción "Activar S/MIME".
SCEP de firma	En la configuración se especifica el perfil SCEP que los dispositivos pueden utilizar para recuperar los certificados necesarios para firmar mensajes de correo mediante S/MIME. Esta configuración es válida únicamente si se ha seleccionado la opción "Activar S/MIME".

iOS: ajuste del perfil de correo	Descripción
Credenciales de usuario de firma	En la configuración se especifica el perfil de credenciales de usuario que los dispositivos pueden utilizar para obtener los certificados de clientes necesarios para firmar mensajes de correo mediante S/MIME. Esta configuración es válida únicamente si se ha seleccionado la opción "Activar S/MIME".
El usuario puede activar y desactivar la firma S/MIME	Esta configuración especifica si un usuario tiene permiso para activar o desactivar la firma S/MIME. Esta configuración se aplica únicamente a dispositivos con iOS 12.0 o versiones posteriores.
El usuario puede cambiar las credenciales de firma	Esta configuración especifica si un usuario puede anular las credenciales de firma. Esta configuración se aplica únicamente a dispositivos con iOS 12.0 o versiones posteriores.
Activar cifrado de mensajes de S/MIME	En la configuración se especifica si desea que un dispositivo cifre los mensajes de correo de salida con el cifrado S/MIME. Esta configuración se aplica únicamente a dispositivos con iOS 10.3 o versiones posteriores.
Credenciales de cifrado	En la configuración se especifica cómo los dispositivos encuentran los certificados necesarios para cifrar los mensajes. Valores posibles: • Certificado compartido • SCEP • Credencial de usuario Después de seleccionar el tipo de perfil, seleccione el certificado compartido, el SCEP o el perfil de credenciales de usuario que desea utilizar. Esta configuración es válida únicamente si se ha seleccionado la opción "Activar S/MIME".
Certificado compartido de cifrado	En la configuración se especifica el perfil de certificado compartido para un certificado de cliente que el dispositivo iOS puede utilizar para cifrar mensajes de correo. Los dispositivos eligen el certificado adecuado para el destinatario para cifrar mensajes mediante S/MIME. Esta configuración es válida únicamente si se ha seleccionado la opción "Activar S/MIME".
SCEP de cifrado	En la configuración se especifica el perfil SCEP que los dispositivos pueden utilizar para recuperar los certificados necesarios para cifrar mensajes de correo mediante S/MIME. Este ajuste se aplica únicamente si se ha seleccionado el ajuste "Activar S/MIME".

iOS: ajuste del perfil de correo	Descripción
Credenciales de usuario de cifrado	En la configuración se especifica el perfil de credenciales de usuario que los dispositivos pueden utilizar para recuperar los certificados de clientes necesarios para cifrar mensajes de correo mediante S/MIME. Este ajuste se aplica únicamente si se ha seleccionado el ajuste "Activar S/MIME".
El usuario puede anular el cifrado S/MIME	Esta configuración especifica si un usuario puede activar o desactivar la configuración de cifrado. Esta configuración se aplica únicamente a dispositivos con iOS 12.0 o versiones posteriores.
El usuario puede anular las credenciales de cifrado S/MIME	Esta configuración especifica si un usuario puede anular las credenciales de cifrado S/MIME. Esta configuración se aplica únicamente a dispositivos con iOS 12.0 o versiones posteriores.
Cifrar mensajes	Esta configuración especifica si se deben cifrar todos los mensajes de correo cuando el usuario los envía (Obligatorio) o si el usuario puede elegir qué mensajes cifrar a la hora de enviarlos (Permitir). Este ajuste se aplica únicamente si se ha seleccionado el ajuste "Activar S/MIME". Valores posibles: • Obligatorio • Permitir El valor predeterminado es "Obligatorio". El requisito mínimo es iOS versión 8.0 y los dispositivos deben estar activados con controles de MDM.
Días para sincronizar	En la configuración se especifica el número de días transcurridos para sincronizar los mensajes de correo y los datos del organizador en un dispositivo iOS. Valores posibles: • 1 día • 3 días • 7 días • 14 días • 1 mes • Indefinidamente El valor predeterminado es "7 días". **Nota:** La configuración se aplica únicamente al correo predeterminado y las aplicaciones del organizador en los dispositivos iOS con el tipo de activación Controles de MDM.
Autenticación	

iOS: ajuste del perfil de correo	Descripción
Activar BlackBerry Secure Gateway	Esta configuración especifica si los dispositivos iOS con el tipo de activación Controles de MDM utilizan BlackBerry Secure Gateway para conectarse al servidor de correo. BlackBerry Secure Gateway proporciona una conexión segura al servidor de correo de su empresa a través de BlackBerry Infrastructure y BlackBerry UEM. Para poder activar este servicio, debe verificar que su empresa tiene las licencias de BlackBerry UEM correspondientes. Para obtener más información, consulte el contenido referente a Licencias. Si ha configurado grupos de servidores para dirigir el tráfico de BlackBerry Secure Gateway a una conexión regional determinada de BlackBerry Infrastructure, debe asociar el perfil de correo electrónico con el grupo de servidores correspondiente.
Tipo de autenticación	En la configuración se especifica el tipo de autenticación que un dispositivo iOS utiliza para conectarse al servidor de correo. Esta configuración es válida únicamente si no se ha seleccionado la opción "Activar BlackBerry Secure Gateway". Valores posibles: • Ninguno • Certificado compartido • SCEP • Credencial de usuario El valor predeterminado es "Ninguno".
Perfil de certificado compartido	En la configuración se especifica el perfil de certificado compartido para un certificado de cliente que el dispositivo iOS utiliza para conectar con el servidor de correo. Esta configuración es válida únicamente si no se ha seleccionado la opción "Activar BlackBerry Secure Gateway" y la opción "Tipo de autenticación" se establece en "Certificado compartido".
Perfil SCEP asociado	En la configuración se especifica el perfil SCEP asociado que un dispositivo iOS debe utilizar para inscribir un certificado de cliente con el objetivo de autenticarlo con el servidor de correo. Esta configuración es válida únicamente si no se ha seleccionado la opción "Activar BlackBerry Secure Gateway" y la opción "Tipo de autenticación" se establece en "SCEP".
Perfil de credenciales de usuario asociado	En la configuración se especifica el perfil de credenciales de usuario asociado que un dispositivo iOS debe utilizar para inscribir un certificado de cliente con el objetivo de autenticarlo con el servidor de correo. Esta configuración es válida únicamente si la opción "Tipo de autenticación" se establece en "Credenciales del usuario".

iOS: ajuste del perfil de correo	Descripción
Utilizar credenciales y certificado	En la configuración se especifica si un dispositivo utiliza las credenciales y un certificado de cliente obtenido mediante el perfil SCEP asociado para autenticar con el servidor de correo. Esta configuración es válida únicamente si no se ha seleccionado la opción "Activar BlackBerry Secure Gateway" y la opción "Tipo de autenticación" se establece en "SCEP".
Utilizar SSL	En la configuración se especifica si un dispositivo debe utilizar SSL para conectarse al servidor de correo.
Aceptar todos los certificados SSL	En esta configuración se especifica si se aceptan todos los certificados SSL.
Dominios de correo electrónico externos	
Lista de dominios de correo externos permitidos	En la configuración se especifica la lista de dominios a los que un usuario puede enviar el correo de trabajo o las entradas de calendario. Por ejemplo, cuando un usuario agrega un destinatario que tiene una dirección de correo en el dominio permitido a un mensaje de correo o a una entrada de calendario, no se muestra ningún mensaje de advertencia. La configuración se aplica solo al espacio de trabajo. Si incluye varios nombres de dominio, sepárelos con una coma (,), un punto y coma (;) o un espacio.
Lista de dominios de correo externos restringidos	En la configuración se especifica la lista de dominios a los que los usuarios no pueden enviar el correo de trabajo o las entradas de calendario. Por ejemplo, si un usuario intenta agregar un destinatario con una dirección de correo del dominio restringido a un mensaje de correo o a una invitación de calendario, la aplicación Work Connect impide que el usuario complete la tarea. La configuración se aplica solo al espacio de trabajo. Si incluye varios nombres de dominio, sepárelos con una coma (,), un punto y coma (;) o un espacio.
Permitir Mail Drop	Esta configuración especifica si los usuarios pueden enviar archivos desde esta cuenta mediante Mail Drop. El requisito mínimo es iOS versión 9.0 y los dispositivos deben estar activados con controles de MDM.

macOS: ajustes del perfil de correo

macOS aplica perfiles a las cuentas de usuario o los dispositivos. Los perfiles de correo se aplican a cuentas de usuario.

macOS: ajuste del perfil de correo	Descripción
Ruta	En la configuración se especifica la ruta de red del servidor de correo.

macOS: ajuste del perfil de correo	Descripción
Puerto	En la configuración se especifica el puerto que se utiliza para conectarse al servidor de correo.
Utilizar SSL	En la configuración se especifica si un dispositivo debe utilizar SSL para conectarse al servidor de correo.
Nombre de host externo o dirección IP	En la configuración se especifica el nombre de host externo o la dirección IP del servidor de correo.
Utilizar SSL externo	En la configuración se especifica si un dispositivo debe utilizar SSL para conectarse al servidor de correo externo.
Ruta externa	En la configuración se especifica la ruta de red del servidor de correo externo.
Puerto del servidor externo	En la configuración se especifica el puerto que se utiliza para conectarse al servidor de correo externo.

Android: ajustes del perfil de correo

Nota: En una futura versión de BlackBerry UEM, la configuración aplicable a BlackBerry Hub + y Dividir productividad se eliminará del perfil de correo y solo estará disponible como una configuración de la aplicación en los ajustes de la misma. En dicha versión, si realiza los ajustes aquí y en la configuración de la aplicación, esta última tendrá prioridad si ambas están asignadas.

Android: ajuste del perfil de correo	Descripción
Configuración de entrega	
Tipo de perfil	En la configuración se especifica si desea que este perfil sea compatible con Exchange ActiveSync o IBM Notes Traveler. Valores posibles: • Exchange ActiveSync • IBM Notes Traveler El valor predeterminado es "Exchange ActiveSync".

Android: ajuste del perfil de correo	Descripción
Días para sincronizar	En la configuración se especifica el número de días transcurridos para sincronizar los mensajes de correo y los datos del organizador en un dispositivo Android. Valores posibles: • Ilimitado • 1 día • 3 días • 7 días • 14 días • 1 mes El valor predeterminado es "1 mes". Para los dispositivos Android que utilizan Samsung KNOX MDM, si establece el valor en Ilimitado, solo se sincroniza un mes. **Nota:** La configuración se aplica únicamente al correo predeterminado y las aplicaciones del organizador en los dispositivos Android con el tipo de activación Controles de MDM. Si al dispositivo se le asigna el tipo de activación Trabajo y personal: privacidad de usuario o Trabajo y personal: control total, la configuración no afecta a la configuración de sincronización para el correo predeterminado y la aplicación del organizador o la aplicación Work Space Manager.
Tipo de autenticación	En la configuración se especifica el tipo de autenticación que un dispositivo Android utiliza para conectarse al servidor de correo. Valores posibles: • Ninguno • Certificado compartido • SCEP • Credencial de usuario El valor predeterminado es "Ninguno".
Perfil SCEP asociado	En la configuración se especifica el perfil SCEP asociado que un dispositivo Android debe utilizar para obtener un certificado de cliente con el objetivo de autenticarlo con el servidor de correo. Esta configuración es válida únicamente si la opción "Tipo de autenticación" se establece en "SCEP".
Utilizar credenciales y certificado	En la configuración se especifica si un dispositivo utiliza las credenciales y un certificado de cliente obtenido mediante el perfil SCEP asociado para autenticar con el servidor de correo. Esta configuración es válida únicamente si la opción "Tipo de autenticación" se establece en "SCEP".

Android: ajuste del perfil de correo	Descripción
Perfil de certificado compartido	En la configuración se especifica el perfil de certificado compartido para un certificado de cliente que el dispositivo Android utiliza para conectar con el servidor de correo. Esta configuración es válida únicamente si la opción "Tipo de autenticación" se establece en "Certificado compartido".
Perfil de credenciales de usuario asociado	En la configuración se especifica el perfil de credenciales de usuario para un certificado de cliente que el dispositivo Android utiliza para conectar con el servidor de correo. Esta configuración es válida únicamente si la opción "Tipo de autenticación" se establece en "Credenciales del usuario".
Utilizar SSL	En la configuración se especifica si un dispositivo debe utilizar SSL para conectarse al servidor de correo.
Aceptar todos los certificados SSL	Esta opción especifica si un dispositivo debe aceptar automáticamente certificados SSL que no sean de confianza procedentes del servidor de correo. Cuando esta opción no está seleccionada, los dispositivos solo se pueden conectar a los servidores de correo que utilizan un certificado SSL de confianza.
Tamaño máximo de archivo adjunto de correo	En la configuración se especifica el tamaño máximo permitido para los archivos adjuntos de correo (en MB). Los valores posibles son de 1 a 365. La configuración predeterminada es 25. La configuración se aplica únicamente a dispositivos Android Enterprise.
Firma de correo predeterminada para los nuevos mensajes	La configuración especifica una firma de correo que se agrega automáticamente a los mensajes de correo nuevos. La configuración se aplica únicamente a dispositivos Android Enterprise.
Activar S/MIME	En la configuración se especifica si los dispositivos pueden enviar mensajes de correo protegidos con S/MIME. Para los dispositivos que utilizan BlackBerry Productivity Suite, debe establecer un valor para la configuración "Compatibilidad de S/MIME" en su lugar.
Firmar mensajes	En la configuración se especifica si desea que los dispositivos envíen todos los mensajes de correo de salida con una firma digital. Esta configuración es válida únicamente si se ha seleccionado la opción "Activar S/MIME". Para los dispositivos Android Enterprise, esta configuración solo se aplica a los dispositivos que utilizan Dividir productividad. Para los dispositivos que utilizan BlackBerry Productivity Suite, debe establecer un valor para la configuración "Mensajes de S/MIME con firma digital" en su lugar.

Android: ajuste del perfil de correo	Descripción
Credenciales de firma	En la configuración se especifican las credenciales que un dispositivo utiliza para firmar los mensajes de correo. Esta configuración es válida únicamente si se ha seleccionado la opción "Firmar mensajes". Valores posibles: • Certificado compartido • SCEP • Credencial de usuario La configuración predeterminada es "Certificado compartido".
Certificado compartido de firma	En la configuración se especifica el perfil de certificado compartido para un certificado de cliente que un dispositivo utiliza para firmar mensajes de correo. Esta configuración es válida únicamente si la opción "Credenciales de firma" se establece en "Certificado compartido".
SCEP de firma	En la configuración se especifica el perfil SCEP para un certificado de cliente que un dispositivo utiliza para firmar mensajes de correo. Esta configuración es válida únicamente si la opción "Credenciales de firma" se establece en "SCEP".
Credenciales de usuario de firma	En la configuración se especifica el perfil de credenciales de usuario para un certificado de cliente que un dispositivo utiliza para firmar mensajes de correo. Esta configuración es válida únicamente si la opción "Credenciales de firma" se establece en "Credenciales del usuario".
Cifrar mensajes	En la configuración se especifica si desea que los dispositivos cifren los mensajes de correo de salida con el cifrado S/MIME. Esta configuración es válida únicamente si se ha seleccionado la opción "Activar S/MIME". Para los dispositivos Android Enterprise, esta configuración solo se aplica a los dispositivos que utilizan Dividir productividad. Para los dispositivos que utilizan BlackBerry Productivity Suite, debe establecer un valor para la configuración "Mensajes de S/MIME con firma digital" en su lugar.

Android: ajuste del perfil de correo	Descripción
Credenciales de cifrado	En la configuración se especifican las credenciales que un dispositivo utiliza para cifrar los mensajes de correo. Esta configuración es válida únicamente si se ha seleccionado la opción "Cifrar mensajes". Valores posibles: • Certificado compartido • SCEP • Credencial de usuario La configuración predeterminada es "Certificado compartido".
Certificado compartido de cifrado	En la configuración se especifica el perfil de certificado compartido para un certificado de cliente que un dispositivo utiliza para cifrar mensajes de correo. Esta configuración es válida únicamente si la opción "Credenciales de cifrado" se establece en "Certificado compartido".
SCEP de cifrado	En la configuración se especifica el perfil SCEP para un certificado de cliente que un dispositivo utiliza para cifrar mensajes de correo. Esta configuración es válida únicamente si la opción "Credenciales de firma" se establece en "SCEP".
Credenciales de usuario de cifrado	En la configuración se especifica el perfil de credenciales de usuario para un certificado de cliente que un dispositivo utiliza para cifrar mensajes de correo. Esta configuración es válida únicamente si la opción "Credenciales de firma" se establece en "Credenciales del usuario".
Requerir autenticación de la tarjeta inteligente para el correo	En la configuración se especifica si se necesita una tarjeta inteligente para los dispositivos Samsung KNOX para autenticar con el servidor de correo.
Permitir al usuario editar la configuración	Especifique si el usuario puede editar la configuración de entrega. La configuración se aplica únicamente a dispositivos Samsung KNOX.
Dominios de correo electrónico externos	
Lista de dominios de correo externos permitidos	En la configuración se especifica la lista de dominios a los que un usuario puede enviar el correo de trabajo o las entradas de calendario. Por ejemplo, cuando un usuario agrega un destinatario que tiene una dirección de correo en el dominio permitido a un mensaje de correo o a una entrada de calendario, no se muestra ningún mensaje de advertencia. La configuración se aplica solo al espacio de trabajo. Si incluye varios nombres de dominio, sepárelos con una coma (,), un punto y coma (;) o un espacio.

Android: ajuste del perfil de correo	Descripción
Lista de dominios de correo externos restringidos	En la configuración se especifica la lista de dominios a los que los usuarios no pueden enviar el correo de trabajo o las entradas de calendario. Por ejemplo, si un usuario intenta agregar un destinatario con una dirección de correo del dominio restringido a un mensaje de correo o a una invitación de calendario, la aplicación Correo o la aplicación Calendario impide que el usuario complete la tarea. La configuración se aplica solo al espacio de trabajo. Si incluye varios nombres de dominio, sepárelos con una coma (,), un punto y coma (;) o un espacio.
BlackBerry Productivity Suite Esta configuración se aplica únicamente a dispositivos Android Enterprise.	
Realizar comprobación OCSP	En la configuración se especifica si los dispositivos usan OCSP para comprobar el estado de los certificados S/MIME.
Permitir que los usuarios acepten certificados que no sean de confianza	En la configuración se especifica si los usuarios pueden permitir que el dispositivo acepte certificados que no sean de confianza.
Permitir el envío de eventos de telemetría desde el perfil de trabajo	En la configuración se especifica si BlackBerry Productivity Suite permite la recopilación de datos de uso.
Tipo de seguridad	En la configuración se especifica el tipo de seguridad que utiliza BlackBerry Productivity Suite. Valores posibles: • SSL • SSL-Trust All El valor predeterminado es "SSL".
Permitir el uso compartido de datos entre perfiles personales y de trabajo	En la configuración se especifica si el perfil personal puede acceder a los datos en el perfil de trabajo. Seleccione esta configuración y la configuración "Permitir que las aplicaciones personales accedan a los datos de trabajo" para activar las siguientes funciones: • Un BlackBerry Hub unificado que contiene tanto las cuentas personales como de trabajo. Para obtener más información, consulte Activación de un BlackBerry Hub unificado. • Un diccionario de teclado unificado que permite que las palabras aprendidas se compartan en perfiles de trabajo y personales. Los usuarios pueden decidir si utilizar el diccionario de teclado unificado para las predicciones y las correcciones. .

Android: ajuste del perfil de correo	Descripción
Permitir que las aplicaciones personales accedan a los datos de trabajo	En la configuración se especifica si las aplicaciones personales pueden acceder a datos de trabajo. Seleccione esta configuración y la configuración "Permitir el uso compartido de datos entre perfiles personales y de trabajo" para activar las siguientes funciones: • Un BlackBerry Hub unificado que contiene tanto las cuentas personales como de trabajo. Para obtener más información, consulte Activación de un BlackBerry Hub unificado. • Un diccionario de teclado unificado que permite que las palabras aprendidas se compartan en perfiles de trabajo y personales. Los usuarios pueden decidir si utilizar el diccionario de teclado unificado para las predicciones y las correcciones.
Configuración S/MIME Esta configuración se aplica únicamente a dispositivos Android Enterprise.	
Compatibilidad de S/MIME	En la configuración se especifica si un dispositivo Android que utiliza BlackBerry Productivity Suite puede enviar mensajes de correo protegidos con S/MIME. Valores posibles: • Permitir • Obligatorio • No permitir El valor predeterminado es "Permitir".
Mensajes de S/MIME con firma digital	En la configuración se especifica si desea que un dispositivo Android que utiliza BlackBerry Productivity Suite envíe mensajes de correo de salida con una firma digital. Valores posibles: • Permitir • Obligatorio • No permitir El valor predeterminado es "Permitir".
Mensajes de S/MIME cifrados	En la configuración se especifica si desea que un dispositivo Android que utiliza BlackBerry Productivity Suite cifre los mensajes de correo de salida con el cifrado S/MIME. Valores posibles: • Permitir • Obligatorio • No permitir El valor predeterminado es "Permitir".

Android: ajuste del perfil de correo	Descripción
Algoritmos de cifrado S/MIME	En la configuración se especifican los algoritmos de cifrado que un dispositivo Android que utiliza BlackBerry Productivity Suite puede utilizar para cifrar mensajes de correo electrónico protegidos con S/MIME. Valores posibles: • AES (256 bits) • AES (192 bits) • AES (128 bits) • Triple DES • ARC2

Windows: ajustes del perfil de correo

Windows: ajuste del perfil de correo	Descripción
Configuración de entrega	
Tipo de perfil	En la configuración se especifica si desea que este perfil sea compatible con Exchange ActiveSync o IBM Notes Traveler. Valores posibles: • Exchange ActiveSync • IBM Notes Traveler El valor predeterminado es "Exchange ActiveSync".
Nombre de cuenta	En la configuración se especifica el nombre de la cuenta de correo de trabajo que aparece en el dispositivo Windows. Puede utilizar una variable como, por ejemplo, %UserEmailAddress%.
Intervalo de sincronización	En la configuración se especifica la frecuencia con que un dispositivo Windows descarga mensajes de correo del servidor de correo. Valores posibles: • A medida que se reciben los elementos • Manual • 15 minutos • 30 minutos • 60 minutos El valor predeterminado es "A medida que se reciben los elementos".

Windows: ajuste del perfil de correo	Descripción
Días para sincronizar	En la configuración se especifica el número de días transcurridos para sincronizar los mensajes de correo y los datos del organizador en un dispositivo Windows. Valores posibles: • Indefinidamente • 3 días • 7 días • 14 días • 1 mes El valor predeterminado es "7 días".
Utilizar SSL	En la configuración se especifica si un dispositivo Windows debe utilizar SSL para conectarse al servidor de correo.
Contenido para sincronizar	
Correo	En la configuración se especifica si desea que un dispositivo Windows sincronice los mensajes de correo con el servidor de correo.
Contactos	En la configuración se especifica si desea que un dispositivo Windows sincronice los contactos con el servidor de correo.
Calendario	En la configuración se especifica si desea que un dispositivo Windows sincronice las entradas de calendario con el servidor de correo.
Tarea	En la configuración se especifica si desea que un dispositivo Windows sincronice los datos de tareas con el servidor de correo. Esta configuración es válida únicamente si la opción "Tipo de perfil" se establece en "Exchange ActiveSync".

Configuración del perfil de correo IMAP/POP3

Puede utilizar una variable en cualquier ajuste de perfil que sea un campo de texto para hacer referencia a un valor en lugar de especificar el valor real. BlackBerry UEM admite variables predeterminadas que son variables predefinidas y personalizadas que se definen. Los perfiles de correo IMAP/POP3 son compatibles con los tipos de dispositivos siguientes:

- iOS
- macOS
- Android
- Windows

En algunos casos, la versión mínima del SO del dispositivo requerida para que sea compatible con una configuración es una versión no admitida por BlackBerry UEM. Para obtener más información acerca de las versiones compatibles, consulte la Matriz de compatibilidad.

Común: configuración del perfil de correo IMAP/POP3

Común: configuración del perfil de correo IMAP/POP3	Descripción
Tipo de correo	Esta configuración especifica el tipo de servidor de correo. Valores posibles: • IMAP • POP3 El valor predeterminado es "IMAP".
Nombre para mostrar	Esta configuración especifica el nombre para mostrar de la cuenta. Si el perfil es para varios usuarios, puede utilizar la variable %UserDisplayName%.
Dirección de correo	En la configuración se especifica la dirección de correo del usuario. Si el perfil es para varios usuarios, puede utilizar la variable %UserEmailAddress%.
Configuración del correo entrante	
Nombre de host o dirección IP	Esta configuración especifica el nombre de host o la dirección IP del servidor de correo para el correo entrante.
Puerto	Esta configuración especifica el puerto que se utiliza para conectarse al servidor de correo para el correo entrante.
Nombre de usuario	En la configuración se especifica el nombre de usuario del usuario. Si el perfil es para varios usuarios, puede utilizar la variable %UserName%.
Utilizar SSL para el correo de entrada	Esta configuración especifica si un dispositivo iOS, Android o Windows Phone debe utilizar SSL para conectarse al servidor de correo con el fin de obtener el correo recibido.
Configuración del correo saliente	
Nombre de host o dirección IP	Esta configuración especifica el nombre de host o la dirección IP del servidor de correo para el correo de salida.
Puerto	Esta configuración especifica el puerto que se utiliza para conectarse al servidor de correo para el correo de salida.
Utilizar SSL para el correo de salida	Esta configuración especifica si un dispositivo iOS, Android o Windows Phone debe utilizar SSL para conectarse al servidor de correo con el fin de enviar correos.
Autenticación requerida para el correo de salida	Esta configuración especifica si un dispositivo debe autenticarse con el servidor para enviar correo.

Común: configuración del perfil de correo IMAP/POP3	Descripción
Utilización de las mismas credenciales que en la configuración de entrada	Esta configuración especifica si un dispositivo iOS, Android o Windows Phone utiliza las mismas credenciales para recibir mensajes de correo que para enviarlos con el fin de autenticarse con el servidor de correo. Si un dispositivo no utiliza las mismas credenciales para recibir mensajes de correo que para enviarlos con el fin de autenticarse con el servidor de correo, puede especificar el nombre de usuario y la contraseña que utiliza dicho dispositivo. Esta configuración solo es válida si la opción "Autenticación requerida para el correo de salida" está seleccionada.

iOS y macOS: configuración del perfil de correo IMAP/POP3

macOS aplica perfiles a las cuentas de usuario o los dispositivos. Los perfiles IMAP/POP3 se aplican a las cuentas de usuario.

iOS: configuración del perfil de correo IMAP/POP3	Descripción
Prefijo de la ruta de acceso de IMAP	Si fuera necesario, esta configuración especifica el prefijo de la ruta de acceso de IMAP. Si fuera necesario, póngase en contacto con su ISP para obtener más información. Esta configuración solo es válida si el valor de la opción "Tipo de correo" se establece en "IMAP".
Permitir que los mensajes se muevan	Esta configuración especifica si desea que los usuarios puedan mover mensajes de correo desde esta cuenta a otra cuenta de correo en un dispositivo iOS.
Permitir la sincronización de direcciones recientes	Esta configuración especifica si un usuario de un dispositivo iOS puede sincronizar direcciones de correo utilizadas recientemente en los dispositivos.
Utilizar solo con correo	En la configuración se especifica si desea que las aplicaciones que no sean la aplicación de correo en el dispositivo iOS puedan utilizar esta cuenta para enviar mensajes de correo.
Activar S/MIME	En la configuración se especifica si un usuario del dispositivo iOS puede enviar mensajes de correo protegidos con S/MIME. S/MIME solo es compatible con dispositivos que se activan con controles de MDM.

iOS: configuración del perfil de correo IMAP/ POP3	Descripción
Credenciales de firma	En la configuración se especifican las credenciales que un dispositivo utiliza para firmar los mensajes de correo. Esta configuración es válida únicamente si se ha seleccionado la opción "Activar S/MIME". Valores posibles: • Certificado compartido • SCEP • Credenciales de usuario La configuración predeterminada es "Certificado compartido".
Certificado compartido de firma	En la configuración se especifica el perfil de certificado compartido para un certificado de cliente que un dispositivo utiliza para firmar mensajes de correo. Esta configuración es válida únicamente si la opción "Credenciales de firma" se establece en "Certificado compartido".
SCEP de firma	En la configuración se especifica el perfil SCEP que los dispositivos pueden utilizar para recuperar los certificados necesarios para firmar mensajes de correo mediante S/MIME. Esta configuración es válida únicamente si la opción "Credenciales de firma" se establece en "SCEP".
Credenciales de usuario de firma	En la configuración se especifica el perfil de credenciales de usuario que los dispositivos pueden utilizar para obtener los certificados de clientes necesarios para firmar mensajes de correo mediante S/MIME. Esta configuración es válida únicamente si la opción "Credenciales de firma" se establece en "Credenciales del usuario".
Credenciales de cifrado	En la configuración se especifica cómo los dispositivos encuentran los certificados necesarios para cifrar los mensajes. Esta configuración es válida únicamente si se ha seleccionado la opción "Activar S/MIME". Valores posibles: • Certificado compartido • SCEP • Credenciales de usuario Después de seleccionar el tipo de perfil, seleccione el certificado compartido, el SCEP o el perfil de credenciales de usuario que desea utilizar.

iOS: configuración del perfil de correo IMAP/ POP3	Descripción
Certificado compartido de cifrado	En la configuración se especifica el perfil de certificado compartido para un certificado de cliente que un dispositivo utiliza para cifrar mensajes de correo. Los dispositivos eligen el certificado adecuado para el destinatario para cifrar mensajes mediante S/MIME. Esta configuración es válida únicamente si la opción "Credenciales de cifrado" se establece en "Certificado compartido".
SCEP de cifrado	En la configuración se especifica el perfil SCEP que los dispositivos pueden utilizar para recuperar los certificados necesarios para cifrar mensajes de correo mediante S/MIME. Esta configuración solo es válida si la opción "Credenciales de cifrado" se establece en "SCEP".
Credenciales de usuario de cifrado	En la configuración se especifica el perfil de credenciales de usuario que los dispositivos pueden utilizar para recuperar los certificados de clientes necesarios para cifrar mensajes de correo mediante S/MIME. Esta configuración solo es válida si la opción "Credenciales de cifrado" se establece en "Credenciales del usuario".
Cifrar mensajes	Esta configuración especifica si se deben cifrar todos los mensajes de correo cuando el usuario los envía (Obligatorio) o si el usuario puede elegir qué mensajes cifrar a la hora de enviarlos (Permitir). Este ajuste se aplica únicamente si se ha seleccionado el ajuste "Activar S/MIME". Valores posibles: • Obligatorio • Permitir El valor predeterminado es "Obligatorio". El requisito mínimo es iOS versión 8.0 y los dispositivos deben estar activados con controles de MDM.
Permitir Mail Drop	Esta configuración especifica si los usuarios pueden enviar archivos desde esta cuenta mediante Mail Drop. El requisito mínimo es iOS versión 9.0 y los dispositivos deben estar activados con controles de MDM.

Android: configuración del perfil de correo IMAP/POP3

Android: configuración del perfil de correo IMAP/POP3	Descripción
Prefijo de la ruta de acceso de IMAP	Si fuera necesario, esta configuración especifica el prefijo de la ruta de acceso de IMAP. Si fuera necesario, póngase en contacto con su ISP para obtener más información. Esta configuración solo es válida si el valor de la opción "Tipo de correo" se establece en "IMAP".
Eliminar correo del servidor	Esta configuración especifica cuándo eliminar un correo desde el servidor de correo. Valores posibles: • Nunca • Al eliminarse de la bandeja de entrada El valor predeterminado es "Nunca". Esta configuración solo es válida si el valor de la opción "Tipo de correo" se establece en "POP3".

Windows: configuración del perfil de correo IMAP/POP3

Windows: configuración del perfil de correo IMAP/POP3	Descripción
Eliminar correo del servidor	En la configuración se especifica cómo se tratan los mensajes de correo cuando un usuario los elimina. Los mensajes de correo pueden eliminarse del servidor (eliminación permanente), o bien, de la bandeja de entrada pero conservarse en la carpeta de la papelera (eliminación temporal). Valores posibles: • Eliminación permanente • Eliminación temporal El valor predeterminado es "Eliminación temporal". Esta configuración solo es válida si el valor de "Tipo de correo" se establece como "IMAP". Esta configuración solo es válida para dispositivos Windows 10.
Dominio	Esta configuración especifica el dominio del servidor de correo.

Windows: configuración del perfil de correo IMAP/POP3	Descripción
Intervalo de sincronización	Esta configuración especifica la frecuencia con que un dispositivo Windows descarga contenido nuevo del servidor de correo. Valores posibles: • Manual • 15 minutos • 30 minutos • 60 minutos • 2 horas El valor predeterminado es "15 minutos".
Cantidad de recuperación inicial	En la configuración se especifica el número de días transcurridos para sincronizar los mensajes de correo y los datos del organizador en un dispositivo Windows. Valores posibles: • Todos • 7 días • 14 días • 30 días El valor predeterminado es "7 días".
Usar solo la red móvil y no Wi-Fi	En la configuración se especifica si los mensajes de correo se envían y reciben solo a través de la red inalámbrica. Esta configuración solo es válida para dispositivos Windows 10.

Ajustes del perfil de Wi-Fi

Puede utilizar una variable en cualquier ajuste de perfil que sea un campo de texto para hacer referencia a un valor en lugar de especificar el valor real. BlackBerry UEM admite variables predeterminadas que son variables predefinidas y personalizadas que se definen. Los perfiles de Wi-Fi son compatibles con los siguientes tipos de dispositivos:

- BlackBerry 10
- iOS
- macOS
- Android
- Windows

En algunos casos, la versión mínima del SO del dispositivo requerida para que sea compatible con una configuración es una versión no admitida por BlackBerry UEM. Para obtener más información acerca de las versiones OS compatibles, consulte la Matriz de compatibilidad.

Común: ajustes del perfil Wi-Fi

Común: ajuste del perfil Wi-Fi	Descripción
SSID	Esta configuración especifica el nombre de una red Wi-Fi y sus puntos de acceso inalámbrico. El SSID distingue mayúsculas de minúsculas y debe contener caracteres alfanuméricos. Los valores posibles están limitados a 32 caracteres.
Red oculta	En la configuración se especifica si la red Wi-Fi oculta el SSID.

BlackBerry 10: ajustes del perfil de Wi-Fi

BlackBerry 10: ajuste del perfil de Wi-Fi	Descripción
Tipo de seguridad	En la configuración se especifica el tipo de seguridad que utiliza la red Wi-Fi. Valores posibles: • Ninguno • WEP personal • WPA-Personal • WPA-Enterprise • WPA2-Personal • WPA2-Enterprise El valor predeterminado es "Ninguno".
Clave WEP	Esta configuración especifica la clave WEP para la red Wi-Fi. La clave WEP debe contener 10 o 26 caracteres hexadecimales (0-9, A-F) o bien 5 o 13 caracteres alfanuméricos (0-9, A-Z). Ejemplos de valores de clave hexadecimal son ABCDEF0123 o ABCDEF0123456789ABCDEF0123. Ejemplos de valores de clave alfanumérica son abCD5 o abCDefGHijKL1. Esta configuración es válida únicamente si la opción "Tipo de seguridad" se establece en "WEP personal".
Tipo de clave previamente compartida	Esta configuración especifica el tipo de clave compartida previamente para la red Wi-Fi. Esta configuración es válida únicamente si la opción "Tipo de seguridad" se establece en "WPA-Personal" o "WPA2-Personal". Valores posibles: • ASCII • HEX El valor predeterminado es "ASCII".

BlackBerry 10: ajuste del perfil de Wi-Fi	Descripción
Clave compartida previamente	Esta configuración especifica la clave compartida previamente para la red Wi-Fi. Esta configuración es válida únicamente si la opción "Tipo de seguridad" se establece en "WPA-Personal" o "WPA2-Personal". Los valores posibles están limitados a 64 caracteres.
Protocolo de autenticación	En la configuración se especifica el método EAP que debe utilizar la red Wi-Fi. Esta configuración es válida únicamente si la opción "Tipo de seguridad" se establece en "WPA-Enterprise" o "WPA2-Enterprise". Valores posibles: • PEAP • TTLS • EAP-FAST • TLS El valor predeterminado es "PEAP".
Autenticación interna	En la configuración se especifica el método de autenticación interna utilizado con un túnel TLS. Si desea utilizar PAP para autenticación interna, establezca la configuración en "Automático". Esta configuración es válida únicamente si la opción "Protocolo de autenticación" se establece en "PEAP" o "TTLS". Valores posibles: • Automático • MS-CHAPv2 • GTC El valor predeterminado es "Automático".
Método de aprovisionamiento EAP-FAST	En la configuración se especifica el método de aprovisionamiento para la autenticación EAP-FAST. Esta configuración es válida únicamente si la opción "Protocolo de autenticación" se establece en "EAP-FAST". Valores posibles: • Anónimo • Autenticado El valor predeterminado es "Anónimo".
Nombre de usuario	En la configuración se especifica el nombre de usuario que un dispositivo BlackBerry 10 debe utilizar para autenticar con la red Wi-Fi. Si el perfil es para varios usuarios, puede especificar la variable %UserName%. Esta configuración es válida únicamente si la opción "Protocolo de autenticación" se establece en "PEAP", "TTLS", "EAP-FAST" o "TLS".

BlackBerry 10: ajuste del perfil de Wi-Fi	Descripción
Contraseña	En la configuración se especifica la contraseña que un dispositivo BlackBerry 10 debe utilizar para autenticar con la red Wi-Fi. Esta configuración es válida únicamente si la opción "Protocolo de autenticación" se establece en "PEAP", "TTLS" o "EAP-FAST".
Tipo de banda	En la configuración se especifica la frecuencia de banda que debe utilizar la red Wi-Fi. Valores posibles: • Dual • 2,4 GHz • 5,0 GHz El valor predeterminado es "Dual".
Activar DHCP	En la configuración se especifica si la red Wi-Fi utiliza DHCP.
Dirección IP	En la configuración se especifica la dirección IP del host de la red Wi-Fi. Esta configuración es válida únicamente si se ha seleccionado la opción "Activar DHCP".
Máscara de subred	En la configuración se especifica la máscara de subred con notación decimal con puntos (por ejemplo, 192.0.2.0). Esta configuración es válida únicamente si se ha seleccionado la opción "Activar DHCP".
DNS primario	En la configuración se especifica el servidor DNS primario con notación decimal con puntos (por ejemplo, 192.0.2.0). Esta configuración es válida únicamente si se ha seleccionado la opción "Activar DHCP".
DNS secundario	En la configuración se especifica el servidor DNS secundario con notación decimal con puntos (por ejemplo, 192.0.2.0). Esta configuración es válida únicamente si se ha seleccionado la opción "Activar DHCP".
Puerta de acceso predeterminada	En la configuración se especifica la puerta de enlace predeterminada con notación decimal con puntos (por ejemplo, 192.0.2.0). Esta configuración es válida únicamente si se ha seleccionado la opción "Activar DHCP".
Sufijo del dominio	Este ajuste especifica la dirección FQDN del sufijo DNS. Esta configuración es válida únicamente si se ha seleccionado la opción "Activar DHCP".
Activar IPv6	En la configuración se especifica si la red Wi-Fi es compatible con IPv6.

BlackBerry 10: ajuste del perfil de Wi-Fi	Descripción
Activar comunicación entre puntos de acceso	Esta configuración especifica si el dispositivo BlackBerry 10 puede establecer comunicaciones Wi-Fi entre puntos de acceso inalámbricos.
El usuario puede editar	En la configuración se especifican los ajustes de Wi-Fi que un usuario de dispositivo BlackBerry 10 puede cambiar. Si la configuración se establece en "Solo lectura", el usuario no podrá cambiar los ajustes. Si la configuración se establece en "Solo credenciales", el usuario podrá cambiar el nombre de usuario y la contraseña. Valores posibles: • Solo lectura • Solo credenciales El valor predeterminado es "Solo lectura".
Nivel de seguridad de datos	En la configuración se especifica el dominio del espacio de trabajo donde se guarda el perfil de Wi-Fi cuando el espacio de trabajo utiliza protección avanzada para los datos almacenados. Este ajuste solo es válido si se ha seleccionado la regla de política de TI "Forzar protección avanzada de los datos almacenados". Si la configuración se establece en "Siempre disponible", el perfil se guarda en el dominio de inicio y está disponible cuando el espacio de trabajo se bloquea. Si la configuración se establece en "Disponible después de autenticación", el perfil se guarda en el dominio operacional y está disponible después de que el espacio de trabajo se haya desbloqueado, hasta que se reinicia el dispositivo. Si la configuración se establece en "Disponible únicamente cuando el espacio de trabajo está desbloqueado", el perfil se guarda en el dominio de bloqueo y puede utilizarse para las conexiones Wi-Fi solo cuando el espacio de trabajo está desbloqueado. Valores posibles: • Siempre disponible • Disponible después de autenticación • Disponible únicamente cuando el espacio de trabajo está desbloqueado El valor predeterminado es "Siempre disponible". El requisito mínimo es BlackBerry 10 OS versión 10.3.1.
Forzar TLS 1.2	En la configuración se especifica si los dispositivos con BlackBerry 10 deben utilizar TLS 1.2 para la comunicación a través de la red Wi-Fi. Valores posibles: • Desactivado • Activado El valor predeterminado es "Desactivado". El requisito mínimo es BlackBerry 10 OS versión 10.3.3.
Confiar	

BlackBerry 10: ajuste del perfil de Wi-Fi	Descripción
Origen del certificado de cliente	En la configuración se especifica el modo en que los dispositivos BlackBerry 10 pueden obtener el certificado de cliente. Hay cuatro opciones para los dispositivos de obtener certificados de cliente: • Si elige "SCEP", también debe especificar el perfil SCEP asociado que el dispositivo puede utilizar para descargar el certificado de cliente. • Si elige "Credenciales del usuario", también debe especificar el perfil de credenciales de usuario que el dispositivo puede utilizar para descargar el certificado de cliente. • Si elige "Tarjeta inteligente", el usuario debe emparejar el dispositivo con una tarjeta inteligente que incluya el certificado de cliente. • Si elige la opción "Otros", el usuario debe agregar el certificado de cliente al dispositivo manualmente. La tarjeta inteligente es compatible con dispositivos con BlackBerry 10 OS versión 10.3.1 y posteriores. Valores posibles: • Tarjeta inteligente • SCEP • Credencial de usuario • Otros El valor predeterminado es "Otros".
Perfil SCEP asociado	En la configuración se especifica el perfil SCEP asociado que un dispositivo BlackBerry 10 debe utilizar para inscribir un certificado de cliente con el objetivo de autenticarlo con la red Wi-Fi. Esta configuración es válida únicamente si la opción "Origen del certificado de cliente" se establece en "SCEP".
Perfil de credenciales de usuario asociado	En la configuración se especifica el perfil de credenciales de usuario asociado que un dispositivo BlackBerry 10 debe utilizar para inscribir un certificado de cliente con el objetivo de autenticarlo con la red Wi-Fi. Esta configuración es válida únicamente si la opción "Origen del certificado de cliente" se establece en "Credenciales del usuario". El requisito mínimo para utilizar un perfil de credenciales de usuario es BlackBerry 10 OS versión 10.3.1.
Origen del certificado de confianza	En la configuración se especifica el origen del certificado de confianza. Si la configuración se establece en "Almacén de certificados de confianza", un dispositivo BlackBerry 10 puede conectarse a la red Wi-Fi que utiliza cualquier certificado del almacén de certificados de Wi-Fi. Valores posibles: • Ninguno • Almacén de certificados de confianza El valor predeterminado es "Ninguno".

BlackBerry 10: ajuste del perfil de Wi-Fi	Descripción
Perfiles asociados	
Utilice un perfil de conectividad de la empresa con una conexión BlackBerry Secure Connect Plus para los datos de trabajo	En la configuración se especifica si todo el tráfico del espacio de trabajo se dirige a través de BlackBerry Secure Connect Plus, aunque los dispositivos BlackBerry 10 puedan acceder a la red Wi-Fi de trabajo. Si no selecciona este ajuste, cuando configure un perfil Wi-Fi y lo asigne a los dispositivos BlackBerry 10, los dispositivos darán prioridad a la red Wi-Fi de trabajo sobre BlackBerry Secure Connect Plus para el tráfico del espacio de trabajo. Si desea utilizar esta característica, en la política de TI que se asigna a los usuarios del dispositivo con BlackBerry 10, compruebe que no se ha seleccionado la regla de política de TI **Forzar control de acceso a la red para las aplicaciones de trabajo**. Este ajuste puede afectar a la utilización de datos y los costes de red de la empresa. Verifique que esta sea la configuración preferida de la empresa antes de utilizar esta característica. El requisito mínimo es BlackBerry 10 OS versión 10.3.2.
Perfil VPN asociado	En la configuración se especifica el perfil VPN asociado que un dispositivo BlackBerry 10 debe utilizar para conectarse a una red VPN cuando el dispositivo está conectado a la red Wi-Fi.
Perfil proxy asociado	En la configuración se especifica el perfil de proxy asociado que un dispositivo BlackBerry 10 debe utilizar para conectarse al servidor proxy cuando el dispositivo está conectado a la red Wi-Fi.

iOS y macOS: configuración de perfil Wi-Fi

macOS aplica perfiles a las cuentas de usuario o los dispositivos. Puede configurar un perfil de Wi-Fi para aplicarlo a una u otra opción.

iOS y macOS: configuración de perfil Wi-Fi	Descripción
Conexión automática a la red	Esta configuración especifica si un dispositivo puede conectarse automáticamente a la red Wi-Fi.
Aplicar perfil a	Esta configuración especifica si el perfil Wi-Fi se aplica a la cuenta de usuario o al dispositivo. Valores posibles: • Usuario • Dispositivo Esta configuración solo es válida para macOS.

iOS y macOS: configuración de perfil Wi-Fi	Descripción
Perfil proxy asociado	En la configuración se especifica el perfil de proxy asociado que un dispositivo debe utilizar para conectarse al servidor proxy cuando el dispositivo está conectado a la red Wi-Fi.
Tipo de red	Esta configuración especifica la configuración para la red Wi-Fi. Las configuraciones del punto de acceso se aplican únicamente a dispositivos iOS y macOS. Para configurar los ajustes de Wi-Fi para los dispositivos BlackBerry, Android, y Windows Phone, cree un perfil de Wi-Fi independiente. Valores posibles: • Estándar • Punto de acceso heredado • Punto de acceso 2.0 El valor predeterminado es "Estándar".
Nombre de operador mostrado	Esta configuración especifica el nombre descriptivo del operador del punto de acceso. Esta configuración es válida únicamente si la opción "Tipo de red" se establece en "Punto de acceso 2.0".
Nombre de dominio	Esta configuración especifica el nombre del dominio del operador del punto de acceso. Esta configuración es válida únicamente si la opción "Tipo de red" se establece en "Punto de acceso 2.0". No se requiere el ajuste "SSID" cuando utiliza este ajuste.
Identificadores de empresa de los consorcios de roaming	En la configuración se especifican los identificadores de empresa de los consorcios de roaming y proveedores de servicios que son accesibles a través del punto de acceso. Esta configuración es válida únicamente si la opción "Tipo de red" se establece en "Punto de acceso 2.0".
Nombres de dominio NAI	En la configuración se especifican los nombres de dominio NAI que pueden autenticar un dispositivo iOS. Esta configuración es válida únicamente si la opción "Tipo de red" se establece en "Punto de acceso 2.0".
MCC/MNC	En la configuración se especifican las combinaciones MCC/MNC que identifican a los operadores de red móvil. Cada valor debe contener exactamente seis dígitos. Esta configuración es válida únicamente si la opción "Tipo de red" se establece en "Punto de acceso 2.0".

iOS y macOS: configuración de perfil Wi-Fi	Descripción
Permitir la conexión a redes de socios de roaming	Esta configuración especifica si un dispositivo puede conectarse a los socios de roaming para obtener un punto de acceso. Esta configuración es válida únicamente si la opción "Tipo de red" se establece en "Punto de acceso 2.0".
Tipo de seguridad	En la configuración se especifica el tipo de seguridad que debe utilizar la red Wi-Fi. Si el ajuste "Tipo de red" se establece en "Punto de acceso 2.0", este ajuste se establece en "WPA2-Enterprise ". Valores posibles: • Ninguna • WEP personal • Empresa con WEP • WPA-Personal • WPA-Enterprise • WPA2-Personal • WPA2-Enterprise El valor predeterminado es "Ninguno".
Clave WEP	Esta configuración especifica la clave WEP para la red Wi-Fi. La clave WEP debe contener 10 o 26 caracteres hexadecimales (0-9, A-F) o bien 5 o 13 caracteres alfanuméricos (0-9, A-Z). Ejemplos de valores de clave hexadecimal son ABCDEF0123 o ABCDEF0123456789ABCDEF0123. Ejemplos de valores de clave alfanumérica son abCD5 o abCDefGHijKL1. Esta configuración es válida únicamente si la opción "Tipo de seguridad" se establece en "WEP personal".
Clave compartida previamente	Esta configuración especifica la clave compartida previamente para la red Wi-Fi. Esta configuración es válida únicamente si la opción "Tipo de seguridad" se establece en "WPA-Personal " o "WPA2-Personal ".
Protocolos	

iOS y macOS: configuración de perfil Wi-Fi	Descripción
Protocolo de autenticación	En la configuración se especifican los métodos EAP que debe admitir la red Wi-Fi. Puede seleccionar múltiples métodos EAP. Esta configuración es válida únicamente si la opción "Tipo de seguridad" se establece en "Empresa con WEP", "WPA-Enterprise " o "WPA2-Enterprise ". Selecciones posibles: • TLS • TTLS • LEAP • PEAP • EAP-FAST • EAP-SIM
Autenticación interna	En la configuración se especifica el método de autenticación interna que desea utilizar con TTLS. Esta configuración es válida únicamente si la opción "Protocolo de autenticación" se establece en "TTLS". Valores posibles: • Ninguna • PAP • CHAP • MS-CHAP • MS-CHAPv2 • EAP El valor predeterminado es "MS-CHAPv2".
Utilizar PAC	En la configuración se especifica si el método EAP-FAST debe utilizar credenciales de acceso protegido. Esta configuración es válida únicamente si la opción "Protocolo de autenticación" se establece en "EAP-FAST".
Proporcionar PAC	En la configuración se especifica si el método EAP-FAST debe permitir el suministro de PAC. Esta configuración es válida únicamente si el "Protocolo de autenticación" se establece en "EAP-FAST" y se selecciona la opción "Utilizar PAC".
Proporcionar PAC de forma anónima	En la configuración se especifica si el método EAP-FAST debe permitir el suministro anónimo de PAC. Esta configuración es válida únicamente si la opción "Protocolo de autenticación" se establece en "EAP-FAST" y se selecciona la opción "Utilizar PAC" y la opción "Proporcionar PAC".
Autenticación	

iOS y macOS: configuración de perfil Wi-Fi	Descripción
Identidad externa para TTLS, PEAP y EAP-FAST	En la configuración se especifica la identidad externa para un usuario enviado en texto no cifrado. Puede especificar un nombre de usuario anónimo para ocultar la identidad real del usuario (por ejemplo, anónimo). El túnel cifrado se utiliza para autenticar el nombre de usuario real con la red Wi-Fi. Si la identidad externa incluye el nombre de dominio kerberos para distribuir la solicitud, debe ser el dominio kerberos real del usuario (por ejemplo, anónimo@ejemplo.com). Esta configuración es válida únicamente si la opción "Protocolo de autenticación" se establece en "TTLS", "PEAP" o "EAP-FAST".
Utilizar contraseña incluida en el perfil de Wi-Fi	En la configuración se especifica si desea que el perfil de Wi-Fi incluya la contraseña para la autenticación. Esta configuración es válida únicamente si la opción "Tipo de seguridad" se establece en "Empresa con WEP", "WPA-Enterprise " o "WPA2-Enterprise ".
Contraseña	En la configuración se especifica la contraseña que un dispositivo iOS debe utilizar para autenticar con la red Wi-Fi. Esta configuración es válida únicamente si se ha seleccionado la opción "Utilizar contraseña incluida en el perfil de Wi-Fi ".
Nombre de usuario	En la configuración se especifica el nombre de usuario que un dispositivo iOS debe utilizar para autenticar con la red Wi-Fi. Si el perfil es para varios usuarios, puede especificar la variable %UserName%. Esta configuración es válida únicamente si la opción "Tipo de seguridad" se establece en "Empresa con WEP", "WPA-Enterprise " o "WPA2-Enterprise ".
Tipo de autenticación	En la configuración se especifica el tipo de autenticación que un dispositivo debe utilizar para conectarse a la red Wi-Fi. Esta configuración es válida únicamente si la opción "Tipo de seguridad" se establece en "Empresa con WEP", "WPA-Enterprise " o "WPA2-Enterprise ". Valores posibles: • Ninguna • Certificado compartido • SCEP • Credenciales de usuario El valor predeterminado es "Ninguno".

iOS y macOS: configuración de perfil Wi-Fi	Descripción
Tipo de vinculación de certificado	En la configuración se especifica el tipo de vínculo para el certificado de cliente asociado al perfil de Wi-Fi. Esta configuración es válida únicamente si la opción "Tipo de autenticación" se establece en "Certificado compartido". Valores posibles: • Referencia única • Inyección variable El valor predeterminado es "Referencia única".
Perfil de certificado compartido	En la configuración se especifica el perfil de certificado compartido con el certificado de cliente que un dispositivo debe utilizar para autenticar con la red Wi-Fi. Esta configuración es válida únicamente si la opción "Tipo de vinculación de certificado" se establece en "Referencia única".
Nombre del certificado de cliente	En la configuración se especifica el nombre del certificado de cliente que un dispositivo debe utilizar para autenticar con la red Wi-Fi. Esta configuración es válida únicamente si la opción "Tipo de vinculación de certificado" se establece en "Inyección variable".
Perfil SCEP asociado	En la configuración se especifica el perfil SCEP asociado que un dispositivo debe utilizar para obtener un certificado de cliente con el objetivo de autenticarlo con la red Wi-Fi. Esta configuración es válida únicamente si la opción "Tipo de autenticación" se establece en "SCEP".
Perfil de credenciales de usuario asociado	En la configuración se especifica el perfil de credenciales de usuario asociado que un dispositivo debe utilizar para obtener un certificado de cliente con el objetivo de autenticarlo con la red Wi-Fi. Esta configuración es válida únicamente si la opción "Tipo de autenticación" se establece en "Credenciales del usuario".
Confiar	
Nombres comunes de certificado esperados por el servidor de autenticación	En la configuración se especifican los nombres comunes en el certificado que el servidor de autenticación debe enviar al dispositivo (por ejemplo, *.example.com). Esta configuración es válida únicamente si la opción "Tipo de seguridad" se establece en "Empresa con WEP", "WPA-Enterprise " o "WPA2-Enterprise ".

iOS y macOS: configuración de perfil Wi-Fi	Descripción
Tipo de vinculación de certificado	En la configuración se especifica el tipo de vinculación para los certificados de confianza asociados al perfil de Wi-Fi. Esta configuración es válida únicamente si la opción "Tipo de seguridad" se establece en "Empresa con WEP", "WPA-Enterprise " o "WPA2-Enterprise ". Valores posibles: • Referencia única • Inyección variable El valor predeterminado es "Referencia única".
Perfiles de certificado de CA	En la configuración se especifican los perfiles de certificado de CA con los certificados de confianza que un dispositivo debe utilizar para establecer una conexión de confianza con una red Wi-Fi. Esta configuración es válida únicamente si la opción "Tipo de vinculación de certificado" se establece en "Referencia única".
Nombres de certificados de confianza	En la configuración se especifica el nombre de los certificados de confianza que un dispositivo debe utilizar para establecer una conexión de confianza con una red Wi-Fi. Esta configuración es válida únicamente si la opción "Tipo de vinculación de certificado" se establece en "Inyección variable".
Confiar en las decisiones de los usuarios	En la configuración se especifica si un dispositivo debe solicitar al usuario que confíe en un servidor cuando no puede establecerse la cadena de confianza. Si no se selecciona este ajuste, solo se permitirán las conexiones a los servidores de confianza que especifique. Esta configuración es válida únicamente si la opción "Tipo de seguridad" se establece en "Empresa con WEP", "WPA-Enterprise " o "WPA2-Enterprise ".
Activar perfil de marcado de QoS	Esta configuración especifica si puede activar el marcado L2 y L3 para el tráfico enviado a través de la red Wi-Fi. Esta configuración solo es válida para dispositivos con iOS 10 y posterior.
Usar QoS para llamadas de FaceTime	Esta configuración especifica si el tráfico de audio y vídeo para llamadas de FaceTime puede utilizar el marcado L2 y L3. Esta configuración solo es válida para dispositivos con iOS 10 y posterior.
Usar solo marcado L2 para tráfico de QoS	Esta configuración especifica si el tráfico enviado a través de la red Wi-Fi solo utiliza el marcado L2. Esta configuración solo es válida para dispositivos con iOS 10 y posterior.
Aplicar marcado de QoS a aplicaciones seleccionadas	Esta configuración especifica los ID de paquete para aplicaciones que pueden utilizar el marcado L2 y L3. Esta configuración solo es válida para dispositivos con iOS 10 y posterior.

Android: ajustes del perfil de Wi-Fi

Android: ajuste del perfil de Wi-Fi	Descripción
Perfil proxy asociado	En la configuración se especifica el perfil de proxy asociado que un dispositivo Android debe utilizar para conectarse al servidor proxy cuando el dispositivo está conectado a la red Wi-Fi. Los dispositivos Android 8.0 y versiones posteriores con Controles de MDM o Privacidad del usuario no son compatibles con perfiles de Wi-Fi con configuración de proxy. Si un dispositivo con uno de estos tipos de activación se actualiza a Android 8.0, los perfiles de Wi-Fi que tienen un perfil de proxy asociado se eliminarán del dispositivo.
BSSID	En la configuración se especifica la dirección MAC de un punto de acceso inalámbrico de la red Wi-Fi.
DNS primario	En la configuración se especifica el servidor DNS primario con notación decimal con puntos (por ejemplo, 192.0.2.0). La configuración se aplica únicamente a los dispositivos que utilizan Samsung KNOX cuando la dirección IP se asigna de forma estática por la red de la empresa.
DNS secundario	En la configuración se especifica el servidor DNS secundario con notación decimal con puntos (por ejemplo, 192.0.2.0). La configuración se aplica únicamente a los dispositivos que utilizan Samsung KNOX cuando la dirección IP se asigna de forma estática por la red de la empresa.
Tipo de seguridad	En la configuración se especifica el tipo de seguridad que debe utilizar la red Wi-Fi. Valores posibles: • Ninguna • Personal • Empresa El valor predeterminado es "Ninguno".
Tipo de seguridad personal	En la configuración se especifica el tipo de seguridad personal que debe utilizar la red Wi-Fi. Esta configuración es válida únicamente si la opción "Tipo de seguridad" se establece en "Personal". Valores posibles: • Ninguna • WEP personal • WPA-Personal/WPA2-Personal El valor predeterminado es "Ninguno".

Android: ajuste del perfil de Wi-Fi	Descripción
Clave WEP	Esta configuración especifica la clave WEP para la red Wi-Fi. La clave WEP debe contener 10 o 26 caracteres hexadecimales (0-9, A-F) o bien 5 o 13 caracteres alfanuméricos (0-9, A-Z). Ejemplos de valores de clave hexadecimal son ABCDEF0123 o ABCDEF0123456789ABCDEF0123. Ejemplos de valores de clave alfanumérica son abCD5 o abCDefGHijKL1. Esta configuración es válida únicamente si la opción "Tipo de seguridad personal" se establece en "WEP personal".
Clave compartida previamente	Esta configuración especifica la clave compartida previamente para la red Wi-Fi. Esta configuración es válida únicamente si la opción "Tipo de seguridad personal" se establece en "WPA-Personal/WPA2-Personal ".
Protocolo de autenticación	En la configuración se especifica el método EAP que debe utilizar la red Wi-Fi. Esta configuración es válida únicamente si la opción "Tipo de seguridad" se establece en "Empresa". Valores posibles: • TLS • TTLS • PEAP • LEAP El valor predeterminado es "TLS". LEAP no es compatible con los dispositivos que utilizan Samsung KNOX.
Autenticación interna	En la configuración se especifica el método de autenticación interna que desea utilizar con TTLS. Esta configuración es válida únicamente si la opción "Protocolo de autenticación" se establece en "TTLS". Valores posibles: • Ninguna • PAP • CHAP • MS-CHAP • MS-CHAPv2 • GTC El valor predeterminado es "MS-CHAPv2". CHAP no es compatible con los dispositivos que utilizan Samsung KNOX.

Android: ajuste del perfil de Wi-Fi	Descripción
Identidad externa de TTLS	En la configuración se especifica la identidad externa para un usuario enviado en texto no cifrado. Puede especificar un nombre de usuario anónimo para ocultar la identidad real del usuario (por ejemplo, anónimo). El túnel cifrado se utiliza para autenticar el nombre de usuario real con la red Wi-Fi. Si la identidad externa incluye el nombre de dominio kerberos para distribuir la solicitud, debe ser el dominio kerberos real del usuario (por ejemplo, anónimo@ejemplo.com). Esta configuración es válida únicamente si la opción "Protocolo de autenticación" se establece en "TTLS".
Identidad externa de PEAP	En la configuración se especifica la identidad externa para un usuario enviado en texto no cifrado. Puede especificar un nombre de usuario anónimo para ocultar la identidad real del usuario (por ejemplo, anónimo). El túnel cifrado se utiliza para autenticar el nombre de usuario real con la red Wi-Fi. Si la identidad externa incluye el nombre de dominio kerberos para distribuir la solicitud, debe ser el dominio kerberos real del usuario (por ejemplo, anónimo@ejemplo.com). Esta configuración es válida únicamente si la opción "Protocolo de autenticación" se establece en "PEAP".
Nombre de usuario	En la configuración se especifica el nombre de usuario que un dispositivo Android debe utilizar para autenticar con la red Wi-Fi. Si el perfil es para varios usuarios, puede especificar la variable %UserName%. Esta configuración es válida únicamente si la opción "Tipo de seguridad" se establece en "Empresa".
Utilizar contraseña incluida en el perfil de Wi-Fi	En la configuración se especifica si desea que el perfil de Wi-Fi incluya la contraseña para la autenticación. Esta configuración es válida únicamente si la opción "Tipo de seguridad" se establece en "Empresa".
Contraseña	En la configuración se especifica la contraseña que un dispositivo Android debe utilizar para autenticar con la red Wi-Fi. Esta configuración es válida únicamente si se ha seleccionado la opción "Utilizar contraseña incluida en el perfil de Wi-Fi ".
Tipo de autenticación	En la configuración se especifica el tipo de autenticación que un dispositivo Android debe utilizar para conectarse a la red Wi-Fi. Esta configuración es válida únicamente si la opción "Tipo de seguridad" se establece en "Empresa". Valores posibles: • Ninguna • Certificado compartido • SCEP • Credenciales de usuario El valor predeterminado es "Ninguno".

Android: ajuste del perfil de Wi-Fi	Descripción
Tipo de vinculación de certificado	En la configuración se especifica el tipo de vínculo para el certificado de cliente asociado al perfil de Wi-Fi. Esta configuración es válida únicamente si la opción "Tipo de autenticación" se establece en "Certificado compartido". Valores posibles: • Referencia única • Inyección variable El valor predeterminado es "Referencia única".
Perfil de certificado compartido	En la configuración se especifica el perfil de certificado compartido con el certificado de cliente que un dispositivo Android debe utilizar para autenticar con la red Wi-Fi. Esta configuración es válida únicamente si la opción "Tipo de vinculación de certificado" se establece en "Referencia única". El nombre del perfil de certificado compartido debe tener menos de 36 caracteres para los dispositivos que utilizan KNOX Workspace.
Perfil SCEP asociado	En la configuración se especifica el perfil SCEP asociado que un dispositivo Android debe utilizar para obtener un certificado de cliente con el objetivo de autenticarlo con la red Wi-Fi. Esta configuración es válida únicamente si la opción "Tipo de autenticación" se establece en "SCEP". El nombre del perfil SCEP debe tener menos de 36 caracteres para los dispositivos que utilizan un KNOX Workspace.
Perfil de credenciales de usuario asociado	En la configuración se especifica el perfil de credenciales de usuario asociado que un dispositivo Android debe utilizar para obtener un certificado de cliente con el objetivo de autenticarlo con la red Wi-Fi. Esta configuración es válida únicamente si la opción "Tipo de autenticación" se establece en "Credenciales del usuario". El nombre del perfil de credenciales de usuario debe tener menos de 36 caracteres para los dispositivos que utilizan un KNOX Workspace.
Nombre del certificado de cliente	En la configuración se especifica el nombre del certificado de cliente que un dispositivo Android debe utilizar para autenticar con la red Wi-Fi. Esta configuración es válida únicamente si la opción "Tipo de vinculación de certificado" se establece en "Inyección variable".
Nombres comunes de certificado esperados por el servidor de autenticación	En la configuración se especifican los nombres comunes en el certificado que el servidor de autenticación debe enviar al dispositivo (por ejemplo, *.example.com). Esta configuración es válida únicamente si la opción "Tipo de seguridad" se establece en "Empresa".

Android: ajuste del perfil de Wi-Fi	Descripción
Tipo de vinculación de certificado	En la configuración se especifica el tipo de vinculación para los certificados de confianza asociados al perfil de Wi-Fi. Esta configuración es válida únicamente si la opción "Tipo de seguridad" se establece en "Empresa". Valores posibles: • Referencia única • Inyección variable El valor predeterminado es "Referencia única".
Perfil de certificado de CA	En la configuración se especifica el perfil de certificado de CA con el certificado de confianza que un dispositivo Android debe utilizar para establecer una conexión de confianza con una red Wi-Fi. Esta configuración es válida únicamente si la opción "Tipo de vinculación de certificado" se establece en "Referencia única".
Nombres de certificados de confianza	En la configuración se especifica el nombre de los certificados de confianza que un dispositivo Android debe utilizar para establecer una conexión de confianza con una red Wi-Fi. Esta configuración es válida únicamente si la opción "Tipo de vinculación de certificado" se establece en "Inyección variable".

Windows: ajustes del perfil de Wi-Fi

Windows: ajuste del perfil de Wi-Fi	Descripción
Conectar automáticamente cuando esta red esté dentro del alcance	Esta configuración especifica si los dispositivos pueden conectarse automáticamente a la red Wi-Fi. Esta configuración es válida para dispositivos con Windows Phone 8.1 y posterior.
Tipo de seguridad	En la configuración se especifica el tipo de seguridad que utiliza la red Wi-Fi. Valores posibles: • Abierta • WPA-Enterprise • WPA-Personal • WPA2-Enterprise • WPA2-Personal El valor predeterminado es "Abierta".

Windows: ajuste del perfil de Wi-Fi	Descripción
Tipo de cifrado	En la configuración se especifica el método de cifrado que utiliza la red Wi-Fi. La configuración "Tipo de seguridad" determina qué tipos de cifrado son compatibles y el valor predeterminado de esta configuración. Valores posibles: • Ninguna • WEP • TKIP • AES
Clave WEP	Esta configuración especifica la clave WEP para la red Wi-Fi. La clave WEP debe contener 10 o 26 caracteres hexadecimales (0-9, A-F) o bien 5 o 13 caracteres alfanuméricos (0-9, A-Z). Ejemplos de valores de clave hexadecimal son ABCDEF0123 o ABCDEF0123456789ABCDEF0123. Ejemplos de valores de clave alfanumérica son abCD5 o abCDefGHijKL1. Esta configuración solo es válida si la opción "Tipo de seguridad" se establece en "Abierta" y el "Tipo de cifrado" en "WEP".
Índice de clave	Esta configuración especifica la posición de la clave coincidente guardada en el punto de acceso inalámbrico. Esta configuración solo es válida si la opción "Tipo de seguridad" se establece en "Abierta" y el "Tipo de cifrado" en "WEP". Los valores posibles son de 1 a 4. El valor predeterminado es 2.
Clave compartida previamente	Esta configuración especifica la clave compartida previamente para la red Wi-Fi. Esta configuración es válida únicamente si la opción "Tipo de seguridad" se establece en "WPA-Personal ".
Activar registro único	Esta configuración especifica si la red Wi-Fi es compatible con la autenticación de registro único. Esta configuración es válida únicamente si la opción "Tipo de seguridad" se establece en "WPA-Enterprise " o "WPA2-Enterprise ".

Windows: ajuste del perfil de Wi-Fi	Descripción
Tipo de registro único	Esta configuración especifica si se ha realizado la autenticación de registro único. Si se establece en "Realizar inmediatamente antes del inicio de sesión del usuario", se realizará el registro único antes de que el usuario inicie sesión en el directorio activo de la empresa. Si se establece en "Realizar inmediatamente después del inicio de sesión del usuario", se realizará el registro único inmediatamente después de que el usuario inicie sesión en el directorio activo de la empresa. Esta configuración solo es válida si se ha seleccionado la opción "Activar registro único". Valores posibles: • Realizar inmediatamente antes del inicio de sesión del usuario • Realizar inmediatamente después del inicio de sesión del usuario El valor predeterminado es "Realizar inmediatamente antes del inicio de sesión del usuario".
Retraso máximo de la conectividad	Esta configuración especifica, en segundos, la demora máxima antes de que falle el intento de conexión de registro único. Esta configuración solo es válida si se ha seleccionado la opción "Activar registro único". Los valores posibles son de 0 a 120 segundos. El valor predeterminado es de "10 segundos".
Permitir que se muestren diálogos adicionales durante el registro único	Esta configuración especifica si un dispositivo puede mostrar cuadros de diálogo a partir de la pantalla de inicio de sesión. Por ejemplo, si un tipo de autenticación EAP requiere que un usuario confirme el certificado enviado por el servidor durante la autenticación, el dispositivo podrá mostrar el cuadro de diálogo. Esta configuración solo es válida si se ha seleccionado la opción "Activar registro único".
Esta red utiliza LAN virtuales independientes para la autenticación de equipo y de usuario	Esta configuración especifica si la VLAN utilizada por un dispositivo cambia en función de la información de inicio de sesión del usuario. Por ejemplo, si el dispositivo se coloca en una VLAN cuando se inicia y, en función de los permisos de usuario, se transfiere a una red VLAN diferente después de que el usuario haya iniciado sesión. Esta configuración solo es válida si se ha seleccionado la opción "Activar registro único".
Validar certificado del servidor	Esta configuración especifica si un dispositivo debe validar el certificado de servidor que comprueba la identidad del punto de acceso inalámbrico. Esta configuración es válida únicamente si la opción "Tipo de seguridad" se establece en "WPA-Enterprise " o "WPA2-Enterprise ".

Windows: ajuste del perfil de Wi-Fi	Descripción
No solicitar al usuario que autorice nuevos servidores ni autoridades de certificación de confianza	Esta configuración especifica si se solicita a un usuario que confíe en el certificado de servidor. Esta configuración solo es válida si la opción "Validar certificado del servidor" está seleccionada.
Perfiles de certificado de CA	Esta configuración especifica el perfil del certificado de CA que proporciona la raíz de confianza del certificado de servidor que utiliza el punto de acceso inalámbrico. Esta configuración limita las CA raíz de las CA seleccionadas en la que confían los dispositivos. Si no se selecciona ninguna CA raíz de confianza, los dispositivos confiarán en todas las CA raíz incluidas en la lista de su almacén de autoridades de certificación raíz de confianza. Esta configuración solo es válida si la opción "Validar certificado del servidor" está seleccionada.
Activar reconexión rápida	Esta configuración especifica si la red Wi-Fi es compatible con la reconexión rápida para la autenticación PEAP a través de varios puntos de acceso inalámbricos. Esta configuración es válida únicamente si la opción "Tipo de seguridad" se establece en "WPA-Enterprise " o "WPA2-Enterprise ".
Ejecutar NAP	Esta configuración especifica si la red Wi-Fi utiliza NAP para realizar comprobaciones de estado del sistema en los dispositivos para verificar que cumplan con los requisitos de salud antes de que se permitan las conexiones a la red. Esta configuración es válida únicamente si la opción "Tipo de seguridad" se establece en "WPA-Enterprise " o "WPA2-Enterprise ".
Activar modo FIPS	Esta opción especifica si la red Wi-Fi es compatible con el cumplimiento del estándar FIPS 140-2. Esta configuración es válida únicamente si la opción "Tipo de seguridad" se establece en "WPA2-Enterprise" o "WPA2-Personal" y si la opción "Tipo de cifrado" se establece en "AES". Esta configuración es válida para dispositivos con Windows Phone 8.1 y posterior.
Activar almacenamiento en caché PMK	Esta configuración especifica si un dispositivo puede guardar la PMK para activar la roaming rápido de WPA2. La roaming rápida ignora los ajustes 802.1X gracias a un punto de acceso inalámbrico que se autenticó previamente en el dispositivo. Esta configuración solo es válida si la opción "Tipo de seguridad" se establece en "WPA2-Enterprise".

Windows: ajuste del perfil de Wi-Fi	Descripción
Tiempo de PMK para activación	Esta configuración especifica el tiempo, en minutos, que un dispositivo puede guardar la PMK en caché. Esta configuración es válida únicamente si se ha seleccionado la opción "Permitir almacenamiento en caché PMK". Los valores posibles oscilan entre 5 y 1440 minutos. El valor predeterminado es de 720 minutos.
Número de entradas en la caché PMK	Esta configuración especifica el número máximo de entradas PMK que un dispositivo puede guardar en caché. Esta configuración es válida únicamente si se ha seleccionado la opción "Permitir almacenamiento en caché PMK". Los valores posibles son de 1 a 255. El valor predeterminado es 128.
Esta red utiliza la autenticación previa	Esta configuración especifica si el punto de acceso es compatible con la autenticación previa de la roaming rápida de WPA2. La autenticación previa permite que los dispositivos que se conectan a un punto de acceso inalámbrico realicen los ajustes 802.1X con otros puntos de acceso inalámbricos dentro de su alcance. La autenticación previa guarda la PMK y la información asociada en la caché PMK. Si el dispositivo se conecta a un punto de acceso inalámbrico con el que se ha autenticado previamente, se utilizará la información de PMK guardada para reducir el tiempo necesario de autenticación y conexión. Esta configuración es válida únicamente si se ha seleccionado la opción "Permitir almacenamiento en caché PMK".
Número máximo de intentos de autenticación previa	Esta configuración especifica el número máximo de intentos de autenticación previa permitido. Esta configuración solo es válida si la opción "Esta red utiliza la autenticación previa" está seleccionada. Los valores posibles son de 1 a 16. El valor predeterminado es 3.
Tipo de proxy	Esta configuración especifica el tipo de configuración de proxy para el perfil Wi-Fi. Configuración posible: • Ninguno • Configuración de PAC • Configuración manual • Autodetección de proxy web La configuración predefinida es "Configuración manual". La configuración se aplica únicamente a dispositivos Windows 10 Mobile.

Windows: ajuste del perfil de Wi-Fi	Descripción
URL de PAC	En la configuración se especifica la URL del servidor web que aloja el archivo de PAC y el nombre del archivo en formato http://<web_server_URL>/<filename>.pac. Esta configuración es válida únicamente si la opción "Tipo de proxy" se establece en "Configuración de PAC".
Dirección	Esta configuración especifica el nombre del servidor y el puerto de la red proxy. Utilice el formato host:puerto (por ejemplo, server01.example.com:123). El host debe ser uno de los siguientes: • Un nombre registrado, como un nombre de servidor, FQDN o nombre de una sola etiqueta (por ejemplo, server01 en lugar de server01.example.com) • Una dirección IPv4 o IPv6 Esta configuración es válida únicamente si la opción "Tipo de proxy" se establece en "Configuración manual".
Autodetección de proxy web	En la configuración se especifica si desea activar el Protocolo de autodescubrimiento de proxy web (WPAD) para la búsqueda de proxy. Esta configuración es válida únicamente si la opción "Tipo de proxy" se establece en "Autodetección de proxy web". De forma predeterminada, esta casilla de verificación no está activada.
Desactivar comprobaciones de conectividad a Internet	En la configuración se especifica si desea desactivar las comprobaciones de conectividad a Internet. De forma predeterminada, esta casilla de verificación no está activada. La configuración se aplica únicamente a dispositivos Windows 10.
Perfil SCEP asociado	En la configuración se especifica el perfil SCEP asociado que un dispositivo debe utilizar para obtener un certificado de cliente con el objetivo de autenticarlo con la red Wi-Fi. La configuración se aplica únicamente a dispositivos Windows 10.

Configuración de perfil VPN

Puede utilizar una variable en cualquier ajuste de perfil que sea un campo de texto para hacer referencia a un valor en lugar de especificar el valor real. BlackBerry UEM admite variables predeterminadas que son variables predefinidas y personalizadas que se definen. Los perfiles de VPN son compatibles con los siguientes tipos de dispositivos:

- BlackBerry 10
- iOS
- macOS
- Samsung KNOX Workspace
- Windows 10

En algunos casos, la versión mínima del SO del dispositivo requerida para que sea compatible con una configuración es una versión no admitida por BlackBerry UEM. Para obtener más información acerca de las versiones OS compatibles, consulte la Matriz de compatibilidad.

BlackBerry 10: ajustes del perfil de VPN

BlackBerry 10: configuración del perfil de VPN	Descripción
Activar VPN a petición	En la configuración se especifica si desea que se active la VPN a petición para el perfil de VPN. Cuando se selecciona este ajuste, puede especificar las aplicaciones que utiliza el perfil de VPN. Solo las aplicaciones que se especifican en este perfil tienen permiso para utilizar este perfil. Para utilizar VPN a petición, asegúrese de que las aplicaciones especificadas se hayan desarrollado para utilizar VPN a petición, las aplicaciones estén asignadas a los usuarios del dispositivo BlackBerry 10 y el perfil de VPN esté asignado a los usuarios de dispositivos. El requisito mínimo es BlackBerry 10 OS versión 10.3.3.
Dirección de servidor	Dicha configuración especifica las direcciones FQDN o IP del servidor VPN.
Tipo de gateway	Esta configuración especifica el tipo de cliente VPN que emula el cliente VPN de un dispositivo BlackBerry 10. Valores posibles: • Check Point VPN-1 • Cisco VPN 3000 Series Concentrator • Cisco Secure PIX Firewall • Cisco IOS Easy VPN • Cisco ASA Series • Cisco AnyConnect • Juniper SRX Series (IPsec VPN) • Juniper MAG Series o Juniper SA Series (SSL VPN) • Servidor VPN Microsoft IKEv2 • Servidor VPN genérico IKEv2 • Servidor VPN en cumplimiento con NIAP IKEv2 El valor predeterminado es "Check Point VPN-1".

BlackBerry 10: configuración del perfil de VPN	Descripción
Tipo de autenticación	En la configuración se especifica el tipo de autenticación para la puerta de enlace VPN. La configuración "Tipo de puerta de enlace" determina qué tipos de autenticación son compatibles y el valor predeterminado de esta configuración. Valores posibles: • PSK • PKI • XAUTH-PSK • XAUTH-PKI • EAP-TLS • EAP-MS-CHAPv2
Clave compartida previamente o contraseña de grupo	En la configuración se especifica la clave compartida previamente o la contraseña de grupo para la puerta de enlace VPN. Esta configuración es válida únicamente si la opción "Tipo de autenticación" se establece en "PSK" o "XAUTH-PSK".
Nombre de usuario	En la configuración se especifica el nombre de usuario que un dispositivo BlackBerry 10 debe utilizar para autenticar con la puerta de enlace VPN. Si el perfil es para varios usuarios, puede utilizar la variable %UserName%. Esta configuración es válida únicamente si la opción "Tipo de puerta de enlace" se establece en "Cisco AnyConnect" o si la opción "tipo de autenticación" se establece en "XAUTH-PSK" o "XAUTH-PKI".
Token de hardware	En la configuración se especifica si un usuario debe utilizar un token de hardware para autenticar con la puerta de enlace VPN. Esta configuración es válida únicamente si la opción "Tipo de autenticación" se establece en "XAUTH-PSK" o "XAUTH-PKI".
Contraseña	En la configuración se especifica la contraseña que un dispositivo BlackBerry 10 debe utilizar para autenticar con la puerta de enlace VPN. Esta configuración es válida únicamente si la opción "Tipo de puerta de enlace" se establece en "Cisco AnyConnect" o si la opción "Tipo de autenticación" se establece en "XAUTH-PSK" o "XAUTH-PKI" y no se selecciona la opción "Token de hardware".
Identidad EAP	En la configuración se especifica la identidad EAP que un dispositivo BlackBerry 10 debe utilizar para autenticar con la puerta de enlace VPN. Esta configuración es válida únicamente si la opción "Tipo de autenticación" se establece en "EAP-TLS".

BlackBerry 10: configuración del perfil de VPN	Descripción
ID de la puerta de enlace EAP-TLS	Esta configuración es válida únicamente si la opción "Tipo de puerta de enlace" se establece en "Servidor VPN en cumplimiento con NIAP IKEv2" o si la opción "Tipo de autenticación" se establece en "EAP-TLS". El requisito mínimo es BlackBerry 10 OS versión 10.3.3.
Identidad MS-CHAPv2 EAP	En la configuración se especifica la identidad EAP de MS-CHAPv2 que un dispositivo BlackBerry 10 debe utilizar para autenticar con la puerta de enlace VPN. Esta configuración es válida únicamente si la opción "Tipo de autenticación" se establece en "EAP-MS-CHAPv2".
Nombre de usuario de MS-CHAPv2	En la configuración se especifica el nombre de usuario de MS-CHAPv2 que un dispositivo BlackBerry 10 debe utilizar para autenticar con la puerta de enlace VPN. Esta configuración es válida únicamente si la opción "Tipo de autenticación" se establece en "EAP-MS-CHAPv2".
Contraseña de MS-CHAPv2	En la configuración se especifica la contraseña de MS-CHAPv2 que un dispositivo BlackBerry 10 debe utilizar para autenticar con la puerta de enlace VPN. Esta configuración es válida únicamente si la opción "Tipo de autenticación" se establece en "EAP-MS-CHAPv2".
Tipo de ID de autenticación	En la configuración se especifica el tipo de ID de autenticación para la puerta de enlace VPN. Esta configuración es válida únicamente si la opción "Tipo de puerta de enlace" se establece en "Juniper MAG Series o Juniper SA Series (SSL VPN)", "Servidor VPN Microsoft IKEv2", "Servidor VPN genérico IKEv2" o "Servidor VPN en cumplimiento con NIAP IKEv2". La configuración "Tipo de puerta de enlace" determina qué tipos de ID de autenticación son compatibles y el valor predeterminado para esta configuración. Valores posibles: • IPv4 • Nombre de dominio completo • Dirección de correo • Nombre distinguido del certificado de identidad • Nombre general del certificado de identidad • ID de clave

BlackBerry 10: configuración del perfil de VPN	Descripción
ID de autenticación o nombre de usuario de grupo	En la configuración se especifica el ID de autenticación o el nombre de usuario de grupo para la puerta de enlace VPN. Esta configuración es válida únicamente si la opción "Tipo de puerta de enlace" se establece en "Juniper MAG Series o Juniper SA Series (SSL VPN)", "Servidor VPN Microsoft IKEv2" o "Servidor VPN genérico IKEv2" o si la opción "Tipo de autenticación" se establece en "PSK" o "XAUTH-PSK".
Tipo de autenticación de gateway	En la configuración se especifica el tipo de autenticación de puerta de enlace para la puerta de enlace VPN. Esta configuración es válida únicamente si la opción "Tipo de puerta de enlace" se establece en "Juniper MAG Series o Juniper SA Series (SSL VPN)", "Servidor VPN Microsoft IKEv2" o "Servidor VPN genérico IKEv2". Valores posibles: • Ninguna • PSK • PKI El valor predeterminado es "Ninguno".
Permitir comprobación OCSP/CRL en los certificados de la red VPN	Esta configuración activa la comprobación de la revocación de los certificados utilizados durante la autenticación. Esta configuración es válida únicamente si la opción "Tipo de puerta de enlace" se establece en "Servidor VPN en cumplimiento con NIAP IKEv2" o si la opción "Tipo de autenticación" se establece en "PKI" o "EAP-TLS". El requisito mínimo es BlackBerry 10 OS versión 10.3.3.
Clave compartida previamente de gateway	En la configuración se especifica la clave compartida previamente de la puerta de enlace VPN. Esta configuración es válida únicamente si la opción "Tipo de autenticación de la puerta de enlace" se establece en "PSK".

BlackBerry 10: configuración del perfil de VPN	Descripción
Tipo de ID de autenticación de la gateway	En la configuración se especifica el tipo de ID de autenticación de puerta de enlace para la puerta de enlace VPN. Esta configuración es válida únicamente si la opción "Tipo de puerta de enlace" se establece en "Juniper MAG Series o Juniper SA Series (SSL VPN)", "Servidor VPN Microsoft IKEv2" o "Servidor VPN genérico IKEv2". Valores posibles: • IPv4 • Nombre de dominio completo • Dirección de correo • Nombre distinguido del certificado de identidad • Nombre general del certificado de identidad • ID de clave El valor predeterminado es "IPv4".
ID de autenticación de la gateway	En la configuración se especifica el ID de autenticación de puerta de enlace para la puerta de enlace VPN. Esta configuración es válida únicamente si la opción "Tipo de ID de autenticación de la puerta de enlace" se establece en "Nombre de dominio completo" o "Dirección de correo".
Envío de ID de solicitud de la puerta de enlace adicional en el mensaje 1 del protocolo IKEv2	El valor predeterminado es Desactivado. Esta configuración es válida únicamente si la opción "Tipo de puerta de enlace" se establece en "Servidor VPN en cumplimiento con NIAP IKEv2". El requisito mínimo es BlackBerry 10 OS versión 10.3.3.
Tipo de ID de la puerta de enlace solicitado	En la configuración se especifica el tipo de ID de puerta de enlace solicitado para la red VPN. Este ajuste es válido únicamente si la opción "Tipo de puerta de enlace" se configura como "Servidor VPN en cumplimiento con NIAP IKEv2" y si se selecciona la opción "Enviar ID de puerta de enlace solicitado en el mensaje 1 del protocolo IKEv2". Valores posibles: • IPv4 • Nombre de dominio completo • Dirección de correo • Nombre distinguido del certificado de identidad • Nombre general del certificado de identidad • ID de clave El valor predeterminado es "IPv4". El requisito mínimo es BlackBerry 10 OS versión 10.3.3.

BlackBerry 10: configuración del perfil de VPN	Descripción
ID de la puerta de enlace solicitado	La configuración solicita un ID de la puerta de enlace específico en el primer mensaje IKE durante el inicio de sesión si el servidor VPN admite varios ID. Puede ser diferente del ID de puerta de enlace utilizado para la autenticación. Este ajuste es válido únicamente si la opción "Tipo de puerta de enlace" se configura como "Servidor VPN en cumplimiento con NIAP IKEv2" y si se selecciona la opción "Enviar ID de puerta de enlace solicitado en el mensaje 1 del protocolo IKEv2". El requisito mínimo es BlackBerry 10 OS versión 10.3.3.
Nombre de usuario secundario	En la configuración se especifica el nombre de usuario que un dispositivo BlackBerry 10 debe utilizar para la autenticación secundaria con la puerta de enlace VPN. Si el perfil es para varios usuarios, puede utilizar la variable %UserName%. Esta configuración es válida únicamente si la opción "Tipo de puerta de enlace" se establece en "Cisco AnyConnect". El requisito mínimo es BlackBerry 10 OS versión 10.3.1.
Contraseña secundaria	En la configuración se especifica la contraseña que un dispositivo BlackBerry 10 debe utilizar para la autenticación secundaria con la puerta de enlace VPN. Esta configuración es válida únicamente si la opción "Tipo de puerta de enlace" se establece en "Cisco AnyConnect". El requisito mínimo es BlackBerry 10 OS versión 10.3.1.
Nombre del grupo	En la configuración se especifica el nombre del grupo para la puerta de enlace VPN. Esta configuración es válida únicamente si la opción "Tipo de puerta de enlace" se establece en "Cisco AnyConnect". El requisito mínimo es BlackBerry 10 OS versión 10.3.1.
Permitir procesamiento automático de certificados de cliente	En la configuración se especifica si un certificado de cliente se selecciona automáticamente cuando se realiza una conexión VPN. Esta configuración es válida únicamente si la opción "Tipo de puerta de enlace" se establece en "Cisco AnyConnect". El requisito mínimo es BlackBerry 10 OS versión 10.3.1.
Permitir autenticación IPsec	En la configuración se especifica si la puerta de enlace VPN debe utilizar la autenticación IPsec. Esta configuración es válida únicamente si la opción "Tipo de puerta de enlace" se establece en "Cisco AnyConnect". El requisito mínimo es BlackBerry 10 OS versión 10.3.1.

BlackBerry 10: configuración del perfil de VPN	Descripción
Tipo de autenticación IPsec	En la configuración se especifica el tipo de autenticación para una conexión VPN IPsec. Esta configuración es válida únicamente si se ha seleccionado la opción "Permitir autenticación IPsec". Valores posibles: • EAP-MS-CHAPv2 • EAP-MD5 • EAP-GTC • EAP-AnyConnect • IKE-RSA El valor predeterminado es "EAP-MS-CHAPv2". El requisito mínimo es BlackBerry 10 OS versión 10.3.1.
ID de autenticación EAP	En la configuración se especifica la identidad EAP que un dispositivo BlackBerry 10 debe utilizar para autenticar con la puerta de enlace VPN. Esta configuración es válida únicamente si la opción "Tipo de autenticación IPSec" se establece en "EAP MSCHAPv2", "EAP MD5" o "EAP GTC".
Excluir subredes	En la configuración se especifica si se debe restringir el acceso a la conexión VPN de subredes específicas. Esta configuración es válida únicamente si la opción "Tipo de puerta de enlace" se establece en "Cisco AnyConnect". El requisito mínimo es BlackBerry 10 OS versión 10.3.1.
Subredes de exclusión	En la configuración se especifican las subredes y máscaras de subred que no se deben enviar a través de la conexión VPN. Esta configuración es válida únicamente si se ha seleccionado la opción "Excluir marcadores de subredes".
Archivo de configuración de Cisco AnyConnect (.xml)	En la configuración se especifica la ubicación del archivo de configuración de Cisco AnyConnect para enviar a los dispositivos BlackBerry 10. Esta configuración es válida únicamente si la opción "Tipo de puerta de enlace" se establece en "Cisco AnyConnect". El requisito mínimo es BlackBerry 10 OS versión 10.3.1.
Permitir aplicaciones personales en redes de trabajo	En la configuración se especifica si desea que las aplicaciones personales de un dispositivo BlackBerry 10 puedan utilizar la conexión VPN. Esta configuración es válida únicamente si se selecciona la regla de política de TI "Permitir que las aplicaciones personales utilicen las redes de trabajo". El requisito mínimo es BlackBerry 10 OS versión 10.3.1.

BlackBerry 10: configuración del perfil de VPN	Descripción
Acción de certificado que no es de confianza	En la configuración se especifica si un dispositivo BlackBerry 10 debe aceptar certificados que no sean de confianza. Si la configuración se establece en "Permitir", el dispositivo aceptará certificados que no sean de confianza automáticamente. Si la configuración se establece en "Preguntar", el usuario podrá elegir si desea aceptar los certificados que no sean de confianza. Si la configuración se establece en "No permitir", el dispositivo no acepta los certificados que no sean de confianza. El ajuste "Tipo de puerta de enlace" determina qué acciones de certificado que no son de confianza son compatibles y el valor predeterminado para este ajuste. Valores posibles: • Permitir • Preguntar • No permitir El requisito mínimo es BlackBerry 10 OS versión 10.3.2.
Origen del certificado de cliente	En la configuración se especifica el modo en que los dispositivos BlackBerry 10 pueden obtener el certificado de cliente. Hay cuatro opciones para los dispositivos de obtener certificados de cliente: • Si elige "Tarjeta inteligente", el usuario debe emparejar el dispositivo con una tarjeta inteligente que incluya el certificado de cliente. • Si elige "SCEP", también debe especificar el perfil SCEP asociado que el dispositivo puede utilizar para descargar el certificado de cliente. • Si elige "Credenciales del usuario", también debe especificar el perfil de credenciales de usuario que el dispositivo puede utilizar para descargar el certificado de cliente. • Si elige la opción "Otros", el usuario debe agregar el certificado de cliente al dispositivo manualmente. La tarjeta inteligente es compatible con dispositivos con BlackBerry 10 OS versión 10.3.1 y posteriores. Esta configuración es válida únicamente si la opción "Tipo de autenticación" se establece en "PKI" o "XAUTH-PKI". Valores posibles: • Tarjeta inteligente • SCEP • Credenciales de usuario • Otros El valor predeterminado es "Otros".

BlackBerry 10: configuración del perfil de VPN	Descripción
Perfil SCEP asociado	En la configuración se especifica el perfil SCEP asociado que un dispositivo BlackBerry 10 debe utilizar para obtener un certificado de cliente con el objetivo de autenticarlo con la VPN . Esta configuración es válida únicamente si la opción "Origen del certificado de cliente" se establece en "SCEP".
Perfil de credenciales de usuario asociado	En la configuración se especifica el perfil de credenciales de usuario asociado que un dispositivo BlackBerry 10 debe utilizar para obtener un certificado de cliente con el objetivo de autenticarlo con la VPN. Esta configuración es válida únicamente si la opción "Origen del certificado de cliente" se establece en "Credenciales del usuario". El requisito mínimo para utilizar un perfil de credenciales de usuario es BlackBerry 10 OS versión 10.3.1.
Duración de IKE	En la configuración se especifica la duración, en segundos, de la conexión IKE. Si establece un valor no admitido o un valor nulo, se usará el valor predeterminado del dispositivo BlackBerry 10. Los valores posibles son de 1 a 2.147.483.647.
Umbral de IKE	La configuración especifica el porcentaje de la duración de IKE al que el cliente VPN iniciará un nuevo intercambio de claves. Valores posibles: 0-100 % El valor predeterminado es "90". Esta configuración es válida únicamente si la opción "Tipo de puerta de enlace" se establece en "Servidor VPN en cumplimiento con NIAP IKEv2". El requisito mínimo es BlackBerry 10 OS versión 10.3.3.
Duración de IPsec	En la configuración se especifica la duración, en segundos, de la conexión IPsec. Si establece un valor no admitido o un valor nulo, se usará el valor predeterminado del dispositivo BlackBerry 10. Los valores posibles son de 1 a 2.147.483.647.
Umbral de IPsec	La configuración especifica el porcentaje del umbral de IPsec al que el cliente VPN iniciará un nuevo intercambio de claves. Valores posibles: 0-100 % El valor predeterminado es "90". Esta configuración es válida únicamente si la opción "Tipo de puerta de enlace" se establece en "Servidor VPN en cumplimiento con NIAP IKEv2". El requisito mínimo es BlackBerry 10 OS versión 10.3.3.

BlackBerry 10: configuración del perfil de VPN	Descripción
Permitir extensiones VPN	En la configuración se permite activar o desactivar las extensiones. Esta configuración es válida únicamente si la opción "Tipo de puerta de enlace" se establece en "Servidor VPN en cumplimiento con NIAP IKEv2". El requisito mínimo es BlackBerry 10 OS versión 10.3.3.
Lista de extensiones VPN	En la configuración se permite especificar una lista de extensiones que se utilizan para generar cargas del ID del proveedor y realizar la validación de certificados adicionales. Este ajuste es válido únicamente si la opción "Tipo de puerta de enlace" se configura como "Servidor VPN en cumplimiento con NIAP IKEv2" y si se selecciona la opción "Permitir extensiones VPN". El requisito mínimo es BlackBerry 10 OS versión 10.3.3.
Requerir extensión de ID de proveedor	En esta configuración se indica que el administrador desea utilizar una de las extensiones de la lista de extensiones VPN para generar una carga del ID del proveedor durante el inicio de sesión. Este ajuste es válido únicamente si la opción "Tipo de puerta de enlace" se configura como "Servidor VPN en cumplimiento con NIAP IKEv2" y si se selecciona la opción "Permitir extensiones VPN". El requisito mínimo es BlackBerry 10 OS versión 10.3.3.
Requerir la extensión de validación de certificados	En esta configuración se indica que el administrador desea utilizar una de las extensiones para realizar la validación de certificados adicionales. Este ajuste es válido únicamente si la opción "Tipo de puerta de enlace" se configura como "Servidor VPN en cumplimiento con NIAP IKEv2" y si se selecciona la opción "Permitir extensiones VPN". El requisito mínimo es BlackBerry 10 OS versión 10.3.3.
Activar la reanudación de la sesión	En la configuración se activan los ajustes de reanudación de la sesión IKEv2. Si el servidor VPN admite esta función, el cliente VPN permitirá suspender y reanudar la sesión en lugar de desconectar y volver a conectar completamente, siempre que la conexión automática VPN esté activada. Esta configuración es válida únicamente si la opción "Tipo de puerta de enlace" se establece en "Servidor VPN en cumplimiento con NIAP IKEv2". El requisito mínimo es BlackBerry 10 OS versión 10.3.3.

BlackBerry 10: configuración del perfil de VPN	Descripción
Umbral de vale	En la configuración se especifica en qué porcentaje de la reanudación de sesión del umbral de vale se producirá la reanudación de la sesión. Valores posibles: 0-100 % El valor predeterminado es "90". Este ajuste es válido únicamente si la opción "Tipo de puerta de enlace" se configura como "Servidor VPN en cumplimiento con NIAP IKEv2" y si se selecciona la opción "Activar reanudación de sesión". El requisito mínimo es BlackBerry 10 OS versión 10.3.3.
Permitir cargas de certificados en formato hash y URL durante el intercambio IKE	En la configuración se especifica si el cliente VPN debe anunciar al servidor VPN que admite el uso de IKEv2 para intercambiar certificados mediante URL y obtener certificados, si están disponibles, desde una URL HTTP facilitada. Este ajuste es válido únicamente si la opción "Tipo de puerta de enlace" se configura como "Servidor VPN en cumplimiento con NIAP IKEv2". El requisito mínimo es BlackBerry 10 OS versión 10.3.3.
Activar el cumplimiento estricto de los algoritmos aprobados	En la configuración se especifica si el uso de algoritmos aprobados por NIAP se aplica estrictamente. Esta configuración es válida únicamente si la opción "Tipo de puerta de enlace" se establece en "Servidor VPN en cumplimiento con NIAP IKEv2". El requisito mínimo es BlackBerry 10 OS versión 10.3.3.
Tunelización dividida	En la configuración se especifica si un dispositivo BlackBerry 10 puede usar la tunelización dividida para omitir la puerta de enlace VPN, siempre que dicha puerta la admita. Este ajuste no es válido si la opción "Tipo de puerta de enlace" se configura como "Servidor VPN en cumplimiento con NIAP IKEv2".
Desactivar banner	En la configuración se especifica si un dispositivo BlackBerry 10 bloquea el banner de VPN. Este ajuste no es válido si la opción "Tipo de puerta de enlace" se configura como "Servidor VPN en cumplimiento con NIAP IKEv2".

BlackBerry 10: configuración del perfil de VPN	Descripción
Origen del certificado de confianza	En la configuración se especifica el origen del certificado de confianza. Si la configuración se establece en "Almacén de certificados de confianza", un dispositivo BlackBerry 10 puede conectarse a la red VPN que utiliza cualquier certificado del almacén de certificados de VPN. Esta configuración es válida únicamente si la opción "Tipo de autenticación" se establece en "PKI" o "XAUTH-PKI". Valores posibles: • Ninguna • Almacén de certificados de confianza El valor predeterminado es "Ninguno".
Determinar IP automáticamente	En la configuración se especifica si un dispositivo BlackBerry 10 debe determinar automáticamente la configuración IP de la puerta de enlace VPN.
IP privada	En la configuración se especifica la IP privada de la puerta de enlace VPN. Esta configuración es válida únicamente si se ha seleccionado la opción "Determinar IP automáticamente".
Máscara de la IP privada	En la configuración se especifica la máscara de la IP privada de la puerta de enlace VPN. Esta configuración es válida únicamente si se ha seleccionado la opción "Determinar IP automáticamente".
Subred	En la configuración se especifica la subred de la puerta de enlace VPN. Esta configuración es válida únicamente si se ha seleccionado la opción "Determinar IP automáticamente".
Máscara de subred	En la configuración se especifica la máscara de subred de la puerta de enlace VPN. Esta configuración es válida únicamente si se ha seleccionado la opción "Determinar IP automáticamente".
Determinar DNS automáticamente	En la configuración se especifica si un dispositivo BlackBerry 10 debe determinar automáticamente la configuración DNS de la puerta de enlace VPN.
DNS primario	En la configuración se especifica el servidor DNS primario con notación decimal con puntos (por ejemplo, 192.0.2.0). Esta configuración es válida únicamente si se ha seleccionado la opción "Determinar DNS automáticamente".

BlackBerry 10: configuración del perfil de VPN	Descripción
DNS secundario	En la configuración se especifica el servidor DNS secundario con notación decimal con puntos (por ejemplo, 192.0.2.0). Esta configuración es válida únicamente si se ha seleccionado la opción "Determinar DNS automáticamente".
Sufijo del dominio	Este ajuste especifica la dirección FQDN del sufijo DNS. Esta configuración es válida únicamente si se ha seleccionado la opción "Determinar DNS automáticamente".
Confidencialidad directa total	En la configuración se especifica si la puerta de enlace VPN debe ser compatible con PFS. Si se selecciona este ajuste, el ajuste "Grupo IPsec DH" no se debe establecer en 0.
Selección manual de algoritmos	En la configuración se especifica si desea establecer algoritmos de cifrado para la puerta de enlace VPN.
Grupo IKE DH	Esta configuración especifica el grupo DH que un dispositivo BlackBerry 10 utiliza para generar el material de clave. Esta configuración es válida únicamente si se ha seleccionado la opción "Selección manual de algoritmos". Valores posibles: • De 1 a 26, excepto 3, 4 y 6 • Personalizar 1 a Personalizar 5 El valor predeterminado es "1".
Personalizar proveedor de IKE DH	En la configuración se especifica el nombre del proveedor para IKE DH personalizado. Esta configuración es válida únicamente si la opción "Grupo IKE DH" se establece en uno de los valores personalizados.
Activar MOBIKE	En la configuración se especifica si la puerta de enlace VPN debe ser compatible con MOBIKE. Esta configuración es válida únicamente si la opción "Tipo de puerta de enlace" se establece en "Servidor VPN Microsoft IKEv2" o "Servidor VPN genérico IKEv2", la opción "Tipo de autenticación" se establece en "PKI" y la opción "Grupo IKE DH" se establece en uno de los valores personalizados. El requisito mínimo es BlackBerry 10 OS versión 10.3.1.

BlackBerry 10: configuración del perfil de VPN	Descripción
Cifrado IKE	En la configuración se especifica el algoritmo que un dispositivo BlackBerry 10 debe utilizar para generar una clave de secreto compartido. Esta configuración es válida únicamente si se ha seleccionado la opción "Selección manual de algoritmos". Valores posibles: • Ninguna • DES (clave de 56 bits) • Triple DES (clave de 168 bits) • AES (clave de 128 bits) • AES (clave de 192 bits) • AES (clave de 256 bits) El valor predeterminado es "Ninguno".
Hash de IKE	En la configuración se especifica la función hash que un dispositivo BlackBerry 10 debe utilizar con IKE. Esta configuración es válida únicamente si se ha seleccionado la opción "Selección manual de algoritmos". Valores posibles: • Ninguna • MD5 • AES-XCBC • SHA-1 • SHA-256 • SHA-384 • SHA-512 El valor predeterminado es "Ninguno".

BlackBerry 10: configuración del perfil de VPN	Descripción
IKE PRF	En la configuración se especifica el PRF que un dispositivo BlackBerry 10 debe utilizar con IKE. Esta configuración es válida únicamente si se ha seleccionado la opción "Selección manual de algoritmos". Valores posibles: • Ninguna • HMAC • HMAC-MD5 • AES-XCBC • HMAC-SHA-1 • HMAC-SHA-256 • HMAC-SHA-384 • HMAC-SHA-512 El valor predeterminado es "Ninguno".
Grupo IPsec DH	En la configuración se especifica el grupo DH que un dispositivo BlackBerry 10 debe utilizar con IPsec. Esta configuración es válida únicamente si se ha seleccionado la opción "Selección manual de algoritmos". Los valores posibles son de 0 a 26, excepto 3, 4 y 6. El valor predeterminado es "0".
Cifrado IPsec	En la configuración se especifica el algoritmo que un dispositivo BlackBerry 10 debe utilizar con IPsec. Esta configuración es válida únicamente si se ha seleccionado la opción "Selección manual de algoritmos". Valores posibles: • Ninguna • DES (clave de 56 bits) • Triple DES (clave de 168 bits) • AES (clave de 128 bits) • AES (clave de 192 bits) • AES (clave de 256 bits) El valor predeterminado es "Ninguno".

BlackBerry 10: configuración del perfil de VPN	Descripción
Hash de IPsec	En la configuración se especifica la función hash que un dispositivo BlackBerry 10 debe utilizar con IPsec. Esta configuración es válida únicamente si se ha seleccionado la opción "Selección manual de algoritmos". Valores posibles: • Ninguna • MD5 • AES-XCBC • SHA-1 • SHA-256 • SHA-384 • SHA-512 El valor predeterminado es "Ninguno".
NAT Keepalive	En la configuración se especifica la frecuencia con la que un dispositivo envía un paquete de NAT Keepalive. Si establece un valor no admitido o un valor nulo, se usará el valor predeterminado del dispositivo BlackBerry 10. Los valores posibles son de 1 a 2.147.483.647.
Frecuencia de DPD	En la configuración se especifica la frecuencia de DPD, en segundos. Un dispositivo BlackBerry 10 admite un ajuste mínimo de 10 segundos. Si establece un valor no admitido o un valor nulo, se usará el valor predeterminado del dispositivo. Los valores posibles son de 1 a 2.147.483.647.
El usuario puede editar	En la configuración se especifican los ajustes de VPN que un usuario de dispositivo BlackBerry 10 puede cambiar. Si la configuración se establece en "Solo lectura", el usuario no podrá cambiar los ajustes. Si la configuración se establece en "Solo credenciales", el usuario podrá cambiar el nombre de usuario y la contraseña. Valores posibles: • Solo lectura • Solo credenciales El valor predeterminado es "Solo lectura".

BlackBerry 10: configuración del perfil de VPN	Descripción
Mostrar información de VPN en el dispositivo	En la configuración se especifica si se muestra la información de VPN en un dispositivo BlackBerry 10. Si la configuración se establece en "Visible", se mostrará la mayor parte de la información del perfil de VPN en el dispositivo. Si la configuración se establece en "Invisible", solo se mostrará el nombre del perfil en el dispositivo. Si la configuración se establece en "Solo credenciales", se mostrarán el nombre de perfil y los campos de credenciales en el dispositivo. Valores posibles: • Visible • Invisible • Solo credenciales El valor predeterminado es "Visible".
Nivel de seguridad de datos	En la configuración se especifica el dominio del espacio de trabajo donde se guarda el perfil de VPN cuando el espacio de trabajo utiliza protección avanzada para los datos almacenados. Este ajuste solo es válido si se ha seleccionado la regla de política de TI "Forzar protección avanzada de los datos almacenados". Si la configuración se establece en "Siempre disponible", el perfil se guarda en el dominio de inicio y está disponible cuando el espacio de trabajo se bloquea. Si la configuración se establece en "Disponible después de autenticación", el perfil se guarda en el dominio operacional y está disponible después de que el espacio de trabajo se haya desbloqueado, hasta que se reinicia el dispositivo. Si la configuración se establece en "Disponible únicamente cuando el espacio de trabajo está desbloqueado", el perfil se guarda en el dominio de bloqueo y puede utilizarse para las conexiones VPN solo cuando el espacio de trabajo está desbloqueado. Valores posibles: • Siempre disponible • Disponible después de autenticación • Disponible únicamente cuando el espacio de trabajo está desbloqueado El valor predeterminado es "Siempre disponible". El requisito mínimo es BlackBerry 10 OS versión 10.3.1.
Perfil proxy asociado	En la configuración se especifica el perfil de proxy asociado que un dispositivo BlackBerry 10 debe utilizar para conectarse al servidor proxy cuando el dispositivo está conectado a la red VPN.

iOS y macOS: configuración del perfil de VPN

macOS aplica perfiles a las cuentas de usuario o los dispositivos. Puede configurar un perfil de VPN para aplicarlo a una u otra opción.

iOS y macOS: configuración del perfil VPN	Descripción
Aplicar perfil a	Esta configuración especifica si el perfil de VPN se aplica a la cuenta de usuario o al dispositivo. Valores posibles: • Usuario • Dispositivo Esta configuración solo es válida para dispositivos macOS.
Tipo de conexión	En la configuración se especifica el tipo de conexión que un dispositivo debe utilizar para una puerta de enlace VPN. Algunos tipos de conexión también requieren que los usuarios instalen la aplicación de VPN correspondiente en el dispositivo. Valores posibles: • L2TP • PPTP • IPsec • Cisco AnyConnect • Juniper • Pulse Secure • F5 • SonicWALL Mobile Connect • Aruba VIA • Check Point Mobile • OpenVPN • Personalizada • IKEv2 El valor predeterminado es "L2TP". Algunos valores no son válidos para los dispositivos macOS.
ID de paquete de VPN	En la configuración se especifica el ID de paquete de la aplicación VPN para una SSL VPN personalizada. El ID de paquete se muestra en formato DNS inverso (por ejemplo, com.ejemplo.VPNapp). Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "Personalizar".
Servidor	Dicha configuración especifica las direcciones FQDN o IP del servidor VPN.
Nombre de usuario	En la configuración se especifica el nombre de usuario que un dispositivo debe utilizar para autenticar con la puerta de enlace VPN. Si el perfil es para varios usuarios, puede especificar la variable %UserName%.

iOS y macOS: configuración del perfil VPN	Descripción
Pares clave-valor personalizados	En la configuración se especifican las claves y los valores asociados de la SSL VPN personalizada. La información de configuración es específica de la aplicación VPN del proveedor. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "Personalizar".
Dominio o grupo de inicio de sesión	En la configuración se especifica el dominio o grupo de inicio de sesión que la puerta de enlace VPN debe utilizar para autenticar un dispositivo iOS. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "SonicWALL Mobile Connect".
Alcance	En la configuración se especifica el nombre del dominio de autenticación que la puerta de enlace VPN debe utilizar para autenticar un dispositivo iOS. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "Juniper" o "Pulse Secure."
Cargo	En la configuración se especifica el nombre de la función de usuario que la puerta de enlace VPN debe utilizar para verificar los recursos de red a los que puede acceder un dispositivo iOS. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "Juniper" o "Pulse Secure".
Tipo de autenticación	En la configuración se especifica el tipo de autenticación para la puerta de enlace VPN. La configuración "Tipo de conexión" determina qué tipos de autenticación son compatibles y el valor predeterminado para esta configuración. Valores posibles: • Contraseña • RSA SecurID • Secreto compartido/Nombre del grupo • Certificado compartido • SCEP • Credencial de usuario
Contraseña	En la configuración se especifica la contraseña que un dispositivo debe utilizar para autenticar con la puerta de enlace VPN. Esta configuración es válida únicamente si la opción "Tipo de autenticación" se establece en "Contraseña".

iOS y macOS: configuración del perfil VPN	Descripción
Nombre del grupo	En la configuración se especifica el nombre del grupo para la puerta de enlace VPN. Este ajuste es válido únicamente en las siguientes condiciones: • El ajuste "Tipo de conexión" se establece en "Cisco AnyConnect". • El ajuste "Tipo de conexión" se establece en "IPsec" y el ajuste "Tipo de autenticación" se establece en "Secreto compartido/Nombre del grupo"
Secreto compartido	En la configuración se especifica el secreto compartido que se utiliza para la autenticación VPN. Este ajuste es válido únicamente en las siguientes condiciones: • El ajuste "Tipo de conexión" se establece en "L2TP". • El ajuste "Tipo de conexión" se establece en "IPsec" y el ajuste "Tipo de autenticación" se establece en "Secreto compartido/Nombre del grupo" • El ajuste "Tipo de conexión" se establece en "IKEv2" y el "Método de autenticación" se establece en "Secreto compartido".
Perfil de certificado compartido	En la configuración se especifica el perfil de certificado compartido con el certificado de cliente que un dispositivo debe utilizar para autenticar con la puerta de enlace VPN. Esta configuración es válida únicamente si la opción "Tipo de autenticación" o la opción "Método de autenticación" se establece en "Certificado compartido".
Perfil SCEP asociado	En la configuración se especifica el perfil SCEP asociado que un dispositivo iOS debe utilizar para obtener un certificado de cliente con el objetivo de autenticarlo con la VPN . Esta configuración es válida únicamente si la opción "Tipo de autenticación" o la opción "Método de autenticación" se establece en "SCEP".
Perfil de credenciales de usuario asociado	En la configuración se especifica el perfil de credenciales de usuario asociado que un dispositivo debe utilizar para obtener un certificado de cliente con el objetivo de autenticarlo con la red VPN. Esta configuración es válida únicamente si la opción "Tipo de autenticación" o la opción "Método de autenticación" se establece en "Credenciales del usuario".

iOS y macOS: configuración del perfil VPN	Descripción
Nivel de cifrado	En la configuración se especifica el nivel de cifrado de datos de la conexión VPN. Si la configuración se establece en "Automática", se permite el uso de todas las intensidades de cifrado disponibles. Si la configuración se establece en "Máxima", solo se permitirá la intensidad de cifrado máxima. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "PPTP". Valores posibles: • Ninguno • Automático • Máximo El valor predeterminado es "Ninguno".
Enrutar tráfico de red a través de VPN	En la configuración se especifica si se enviará todo el tráfico de red a través de la conexión VPN. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "L2TP" o "PPTP".
Usar autenticación híbrida	En la configuración se especifica si se utilizará un certificado de servidor para la autenticación. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "IPsec" y el "Tipo de autenticación" se establece en "Secreto compartido/Nombre del grupo"
Solicitar contraseña	En la configuración se especifica si un dispositivo debe solicitar una contraseña al usuario. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "IPsec" y el "Tipo de autenticación" se establece en "Secreto compartido/Nombre del grupo"
Solicitar PIN de usuario	En la configuración se especifica si el dispositivo debe solicitar un PIN al usuario. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "IPsec" y la opción "Tipo de autenticación" se establece en "Certificado compartido", en "SCEP" o en "Credenciales del usuario".
Dirección remota	En la configuración se especifica las direcciones IP o el nombre de host del servidor VPN. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "IKEv2".

iOS y macOS: configuración del perfil VPN	Descripción
ID local	En la configuración se especifica la identidad del cliente IKEv2 en uno de los siguientes formatos: FQDN, FQDN de usuario, Dirección y ASN1DN. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "IKEv2".
ID remoto	En la configuración se especifica el identificador remoto del cliente IKEv2 con uno de los formatos siguientes: FQDN, FQDN de usuario, Dirección o ASN1DN. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "IKEv2".
Método de autenticación	En la configuración se especifica el método de autenticación para la VPN. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "IKEv2". Valores posibles: • Secreto compartido • Certificado compartido • SCEP • Credencial de usuario
Activar VPN a petición	En la configuración se especifica si un dispositivo puede iniciar automáticamente una conexión VPN al acceder a determinados dominios. En dispositivos iOS, esta configuración se aplica a las aplicaciones de trabajo. Este ajuste es válido únicamente en las siguientes condiciones: • El ajuste "Tipo de conexión" se establece en "IPsec", "Cisco AnyConnect," "Juniper", "Pulse Secure", "F5", "SonicWALL Mobile Connect", "Aruba VIA", "Check Point Mobile", "OpenVPN" o "Personalizada" y el ajuste "Tipo de autenticación" se establece en "Certificado compartido", en "SCEP" o en "Credenciales del usuario". • El ajuste "Tipo de conexión" se establece en "IKEv2" y el "Método de autenticación" se establece en "Certificado compartido".
Nombres de host o dominio que pueden usar VPN a petición	En la configuración se especifican los dominios y las acciones asociadas a VPN a petición. Esta configuración es válida únicamente si se ha seleccionado la opción "Activar VPN a petición". Los valores posibles para "Acción a petición": • Establecer siempre • Establecer si es necesario • No establecer nunca

iOS y macOS: configuración del perfil VPN	Descripción
Reglas de VPN a petición para iOS 7.0 y posteriores	En la configuración se especifican los requisitos de la conexión para VPN a petición. Debe utilizar una o más claves del ejemplo de formato de carga. La configuración anula el ajuste "Nombres de host o dominio que pueden usar VPN a petición". Esta configuración es válida únicamente si se ha seleccionado la opción "Activar VPN a petición".
Permitir autenticación ampliada	En la configuración se especifica si la VPN debe ser compatible con xAuth. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "IKEv2" o "IKEv2 siempre activado".
Versión mínima de TLS	Esta configuración especifica la versión mínima de TLS que los dispositivos que ejecutan iOS 11 y versiones posteriores utilizan para la autenticación EAP-TLS. Esta configuración es válida únicamente si se selecciona la configuración Activar xAuth y el Tipo de autenticación es "Certificado". Valores posibles: • 1.0 • 1.1 • 1.2 La configuración predeterminada es "1.0".
Versión máxima de TLS	Esta configuración especifica la versión máxima de TLS que los dispositivos que ejecutan iOS 11 y versiones posteriores utilizan para la autenticación EAP-TLS. Esta configuración es válida únicamente si se selecciona la configuración Activar xAuth y el Tipo de autenticación es "Certificado". Valores posibles: • 1.0 • 1.1 • 1.2 La configuración predeterminada es "1.2".

iOS y macOS: configuración del perfil VPN	Descripción
Intervalo de Keepalive	En la configuración se especifica la frecuencia con la que un dispositivo envía un paquete Keepalive. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "IKEv2". Valores posibles: • Desactivado • 30 minutos • 10 minutos • 1 minuto La configuración predeterminada es "10 minutos".
Desactivar MOBIKE	En la configuración se especifica si MOBIKE está desactivado. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "IKEv2". El requisito mínimo para los dispositivos iOS es iOS 9.
Desactivar redirección de IKEv2	En la configuración se especifica si la redirección de IKEv2 está desactivada. Si la configuración no está seleccionada, la conexión IKEv2 se redirecciona si se recibe una solicitud de redirección del servidor. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "IKEv2". El requisito mínimo para los dispositivos iOS es iOS 9.
Activar confidencialidad directa total	En la configuración se especifica si la puerta de enlace VPN debe ser compatible con PFS. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "IKEv2". El requisito mínimo para los dispositivos iOS es iOS 9.
Activar NAT Keepalive	En la configuración se especifica si la puerta de enlace VPN debe ser compatible con paquetes de NAT Keepalive. Los paquetes Keepalive se utilizan para mantener las asignaciones NAT para conexiones IKEv2. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "IKEv2". El requisito mínimo para los dispositivos iOS es iOS 9.

iOS y macOS: configuración del perfil VPN	Descripción
Intervalo de NAT Keepalive	En la configuración se especifica la frecuencia con la que un dispositivo envía un paquete de NAT Keepalive (en segundos). Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "IKEv2" y si se selecciona la opción "Activar NAT Keepalive". El valor mínimo y el valor predeterminado son 20. El requisito mínimo para los dispositivos iOS es iOS 9.
Usar subredes internas IKEv2 IPv4 e IPv6	En la configuración se especifica si la VPN puede utilizar los atributos de configuración IKEv2 INTERNAL_IP4_SUBNET e INTERNAL_IP6_SUBNET. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "IKEv2". El requisito mínimo para los dispositivos iOS es iOS 9.
Nombre común del certificado de servidor	En la configuración se especifica el nombre común en el certificado que el servidor IKE debe enviar al dispositivo. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "IKEv2".
Nombre común del emisor del certificado de servidor	En la configuración se especifica el nombre común del emisor del certificado en el certificado que el servidor IKE debe enviar al dispositivo. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "IKEv2".
Aplicar parámetros de asociación de seguridad secundarios	En la configuración se especifica si desea aplicar parámetros de asociación de seguridad secundarios. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "IKEv2".
Aplicar parámetros de asociación de seguridad IKE	En la configuración se especifica si desea aplicar parámetros de asociación de seguridad IKE. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "IKEv2".

iOS y macOS: configuración del perfil VPN	Descripción
Grupo DH	Esta configuración especifica el grupo DH que un dispositivo utiliza para generar el material de clave. Esta configuración es válida únicamente si la opción "Aplicar parámetros de asociación de seguridad secundarios" o "Aplicar parámetros de asociación de seguridad IKE" está seleccionada. Valores posibles: • 0 • 1 • 2 • 5 • 14 • 15 • 16 • 17 • 18 La configuración predeterminada es "2".
Algoritmo de cifrado	En la configuración se especifica el algoritmo de cifrado IKE. Esta configuración es válida únicamente si la opción "Aplicar parámetros de asociación de seguridad secundarios" o "Aplicar parámetros de asociación de seguridad IKE" está seleccionada. Valores posibles: • DES • 3DES • AES 128 • AES 256 La configuración predeterminada es "3DES".
Algoritmo de integridad	En la configuración se especifica el algoritmo de integridad IKE. Esta configuración es válida únicamente si la opción "Aplicar parámetros de asociación de seguridad secundarios" o "Aplicar parámetros de asociación de seguridad IKE" está seleccionada. Valores posibles: • SHA1 96 • SHA1 160 • SHA1 256 • SHA2 384 • SHA2 512 El valor predeterminado es "SHA1-96".

iOS y macOS: configuración del perfil VPN	Descripción
Intervalo para regenerar claves	En la configuración se especifica la duración de la conexión IKE. Esta configuración es válida únicamente si la opción "Aplicar parámetros de asociación de seguridad secundarios" o "Aplicar parámetros de asociación de seguridad IKE" está seleccionada. Los valores posibles son de 10 a 1440 minutos. El valor predeterminado es 1440.
Activar VPN por aplicación	En la configuración se especifica si la puerta de enlace VPN debe ser compatible con VPN por aplicación. Esta característica ayuda a disminuir la carga sobre una VPN de la empresa. Por ejemplo, puede activar que solo un determinado tráfico de trabajo utilice la VPN, por ejemplo, al acceder a servidores de aplicaciones o páginas web detrás del firewall. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "Cisco AnyConnect", "Juniper", "Pulse Secure", "F5", "SonicWALL Mobile Connect", "Aruba VIA", "Check Point Mobile", "OpenVPN", "Personalizar" o "IKEv2".
Permitir la conexión automática de aplicaciones	En la configuración se especifica si las aplicaciones asociadas a VPN por aplicación pueden iniciar automáticamente la conexión VPN. Esta configuración es válida únicamente si se ha seleccionado la opción "Activar VPN por aplicación".
Dominios de Safari	En la configuración se especifica el dominio que puede iniciar la conexión VPN en Safari. Esta configuración es válida únicamente si se ha seleccionado la opción "Activar VPN por aplicación".
Tunelización de tráfico	En la configuración se especifica si la VPN tuneliza el tráfico en la capa de aplicación o la capa IP. Esta configuración es válida únicamente si se ha seleccionado la opción "Activar VPN por aplicación". Valores posibles: • Capa de aplicación • Capa IP La configuración predeterminada es "Capa de aplicación".
Perfil proxy asociado	En la configuración se especifica el perfil de proxy asociado que un dispositivo iOS debe utilizar para conectarse al servidor proxy cuando el dispositivo está conectado a la red VPN.

Android: ajustes del perfil de VPN

Las siguientes configuraciones del perfil VPN solo son compatibles con dispositivos Samsung KNOX Workspace.

Para obtener más información sobre las configuración de perfil VPN compatibles con los dispositivos Samsung KNOX Workspace, consulte Parámetros JSON VPN de Samsung KNOX.

Android: configuración del perfil de VPN	Descripción
Dirección de servidor	Dicha configuración especifica las direcciones FQDN o IP del servidor VPN.
Tipo de VPN	En la configuración se especifica si el dispositivo debe utilizar IPsec o SSL para conectarse al servidor VPN. Valores posibles: • IPsec • SSL El valor predeterminado es "IPsec". La aplicación VPN de Juniper solo admite "SSL".
Autenticación de usuario requerida	En la configuración se especifica si un usuario del dispositivo debe proporcionar un nombre de usuario y una contraseña para conectarse al servidor VPN.
Nombre de usuario	En la configuración se especifica el nombre de usuario que un dispositivo debe utilizar para autenticar con la puerta de enlace VPN. Si el perfil es para varios usuarios, puede utilizar la variable %UserName%. Esta configuración es válida únicamente si se ha seleccionado la opción "Autenticación de usuario requerida".
Contraseña	En la configuración se especifica la contraseña que un dispositivo debe utilizar para autenticar con la puerta de enlace VPN. Esta configuración es válida únicamente si se ha seleccionado la opción "Autenticación de usuario requerida".
Tipo de túnel dividido	En la configuración se especifica si un dispositivo puede usar la tunelización dividida para omitir la puerta de enlace VPN, siempre que esta la admita. Valores posibles: • Desactivado • Manual • Automático Si el ajuste "Tipo de VPN" se establece en "IPsec", este ajuste se debe establecer en "Desactivado". El valor predeterminado es "Desactivado".
Rutas de reenvío	En la configuración se especifica la ruta o rutas que omiten la puerta de enlace VPN. Puede especificar una o más direcciones IP. La configuración es válida únicamente si el ajuste "Tipo de VPN" se establece en "SSL" y el ajuste "Tipo de túnel dividido" se establece en "Manual".

Android: configuración del perfil de VPN	Descripción
DPD	En la configuración se especifica si DPD está activado. Esta configuración es válida únicamente si la opción "Tipo de VPN" se establece en "IPsec".
Versión de IKE	En la configuración especifica la versión del protocolo IKE que debe utilizar con la conexión VPN. Valores posibles: • IKEv1 • IKEv2 El valor predeterminado es "IKEv1". Esta configuración es válida únicamente si la opción "Tipo de VPN" se establece en "IPsec".
Tipo de autenticación IPsec	En la configuración se especifica el tipo de autenticación para la conexión VPN IPsec. La configuración "Versión de IKE" determina qué tipos de autenticación IPsec son compatibles y el valor predeterminado para esta configuración. Valores posibles: • Certificado • Clave compartida previamente • EAP MD5 • EAP MSCHAPv2 • RSA híbrida • Autenticación basada en CAC Esta configuración es válida únicamente si la opción "Tipo de VPN" se establece en "IPsec".
Tipo de ID de grupo IPsec	En la configuración se especifica el tipo de ID de grupo IPsec para VPN. La configuración "Tipo de autenticación IPsec" determina qué tipos de ID de grupo IPsec son compatibles y el valor predeterminado para esta configuración. Valores posibles: • Predeterminado • Dirección IPv4 • Nombre de dominio completo • FQDN de usuario • ID de clave IKE Si la configuración de "Tipo de autenticación IPsec" es "Certificado", la configuración se establece automáticamente en "Predeterminada". Esta configuración es válida únicamente si la opción "Tipo de VPN" se establece en "IPsec".

Android: configuración del perfil de VPN	Descripción
ID de grupo IPsec	En la configuración se especifica el ID de grupo IPsec para VPN. Esta configuración es válida únicamente si la opción "Tipo de VPN" se establece en "IPsec".
Modo de intercambio de clave IKE fase 1	En la configuración se especifica el modo de intercambio para VPN. Valores posibles: • Modo principal • Modo agresivo El valor predeterminado es "Modo principal". Esta configuración es válida únicamente si la opción "Tipo de VPN" se establece en "IPsec".
Duración de IKE	En la configuración se especifica la duración, en segundos, de la conexión IKE. Si establece un valor no admitido o un valor nulo, se usará el valor predeterminado del dispositivo. Esta configuración es válida únicamente si la opción "Tipo de VPN" se establece en "IPsec".
Algoritmo de cifrado IKE	En la configuración se especifica el algoritmo de cifrado utilizado para la conexión IKE. Esta configuración es válida únicamente si la opción "Tipo de VPN" se establece en "IPsec".
Algoritmo de integridad IKE	En la configuración se especifica el algoritmo de integridad utilizado para la conexión IKE. Esta configuración solo es válida si la opción "Tipo de VPN" se establece en "IPsec" y la "Versión IKE", en "IKEv2".
Grupo IPsec DH	Esta configuración especifica el grupo DH que un dispositivo utiliza para generar el material de clave. Los valores posibles son 0, 1, 2, 5, y de 14 a 26. El valor predeterminado es 0. Esta configuración es válida únicamente si la opción "Tipo de VPN" se establece en "IPsec".
Parámetro IPsec	En la configuración se especifica el parámetro IPsec utilizado para la conexión VPN. Esta configuración es válida únicamente si la opción "Tipo de VPN" se establece en "IPsec".

Android: configuración del perfil de VPN	Descripción
Confidencialidad directa total	En la configuración se especifica si la puerta de enlace VPN debe ser compatible con PFS. Esta configuración es válida únicamente si la opción "Tipo de VPN" se establece en "IPsec".
Activar MOBIKE	En la configuración se especifica si la puerta de enlace VPN debe ser compatible con MOBIKE. Esta configuración es válida únicamente si la opción "Tipo de VPN" se establece en "IPsec".
Duración de IPsec	En la configuración se especifica la duración, en segundos, de la conexión IPsec. Si establece un valor no admitido o un valor nulo, se usará el valor predeterminado del dispositivo. Esta configuración es válida únicamente si la opción "Tipo de VPN" se establece en "IPsec".
Algoritmo de cifrado IPsec	En la configuración se especifica el algoritmo de cifrado IPsec utilizado para la conexión VPN. Esta configuración es válida únicamente si la opción "Tipo de VPN" se establece en "IPsec".
Algoritmo de integridad IPsec	En la configuración se especifica el algoritmo de integridad IPsec utilizado para la conexión VPN. Esta configuración solo es válida si la opción "Tipo de VPN" se establece en "IPsec" y la "Versión IKE", en "IKEv2".
Tipo de autenticación	En la configuración se especifica el tipo de autenticación para la puerta de enlace VPN. Valores posibles: • Ninguno • Autenticación basada en certificados • Autenticación basada en CAC El valor predeterminado es "Ninguno". Esta configuración es válida únicamente si la opción "Tipo de VPN" se establece en "SSL".
Algoritmo SSL	En la configuración se especifica el algoritmo de cifrado necesario para la conexión VPN SSL. Esta configuración es válida únicamente si la opción "Tipo de VPN" se establece en "SSL".

Android: configuración del perfil de VPN	Descripción
Agregar información de UID/PID	En la configuración se especifica si se agregará información de UID y PID a los paquetes que se envían a la aplicación de cliente VPN. La configuración se debe seleccionar para la aplicación VPN de Cisco AnyConnect.
Cadenas compatibles	En la configuración se especifica cómo se admite la cadena VPN. Valores posibles: • Cadenas compatibles • Túnel exterior • Túnel interior El valor predeterminado es "Cadenas compatibles".
Tipo de entrada de cadena de proveedor	Esta configuración especifica los pares clave-valor o cadena JSON para la VPN. La información de configuración es específica de la aplicación VPN del proveedor. Valores posibles: • Pares clave-valor de proveedor • Valor de JSON de proveedor El valor predeterminado es "Pares clave-valor de proveedor".
Pares clave-valor de proveedor	En la configuración se especifican las claves y los valores asociados de VPN. La información de configuración es específica de la aplicación VPN del proveedor. Esta configuración es válida únicamente si la configuración "Tipo de entrada de cadena de proveedor" se establece en "Pares clave-valor de proveedor".
Valor de JSON de proveedor	Esta configuración especifica la información de configuración específica de la aplicación VPN del proveedor en formato .json. Esta configuración es válida únicamente si la configuración "Tipo de entrada de cadena de proveedor" se establece en "Valor de JSON de proveedor".
ID de paquete de cliente VPN	En la configuración se especifica el ID de paquete de la aplicación VPN.
Reintentar automáticamente la conexión tras un error	En la configuración se especifica si la conexión VPN se debería reiniciar automáticamente después de que se haya perdido la conexión.
Activar modo FIPS	En la configuración se especifica si el modo FIPS está activado. La activación del modo FIPS garantiza que solo se utilicen algoritmos de cifrado validados por FIPS para la conexión VPN.

Android: configuración del perfil de VPN	Descripción
Conectividad de la empresa para dispositivos Android con un espacio de trabajo	Esta configuración especifica si los dispositivos Samsung KNOX Workspace utilizan una conexión VPN para todas las aplicaciones del espacio de trabajo o solo para las aplicaciones especificadas. • "VPN de todo el contenedor" utiliza una conexión VPN para todas las aplicaciones del espacio de trabajo en el dispositivo. • "VPN por aplicación" utiliza una conexión VPN solo para aplicaciones específicas.
Aplicaciones que pueden utilizar la conexión VPN	Esta configuración especifica las aplicaciones del espacio de trabajo que pueden utilizar una conexión VPN. Puede seleccionar aplicaciones en una lista de aplicaciones disponibles o especificar el ID de paquete de aplicación. Esta configuración es válida únicamente si la configuración "Conectividad de la empresa para dispositivos Android con un espacio de trabajo" se establece en "VPN por aplicación".
Perfil proxy asociado	Esta configuración especifica el perfil de proxy asociado que un dispositivo debe utilizar para conectarse al servidor proxy cuando el dispositivo está conectado a la red VPN.

Referencia relacionada

iOS y macOS: configuración del perfil de VPN
Windows 10: ajustes del perfil de VPN

Windows 10: ajustes del perfil de VPN

Windows: configuración del perfil de VPN	Descripción
Tipo de conexión	En la configuración se especifica el tipo de conexión que un dispositivo Windows 10 debe utilizar para una VPN. Valores posibles: • Microsoft • Junos Pulse • SonicWALL Mobile Connect • F5 • Check Point Mobile • Definición de conexión manual El valor predeterminado es "Microsoft".

Windows: configuración del perfil de VPN	Descripción
Servidor	En la configuración se especifica el nombre DNS o la dirección IP pública o enrutable para la puerta de enlace VPN. La configuración puede señalar a la IP externa de una VPN o a una IP virtual de una granja de servidores. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "Microsoft".
Lista de URL de servidores	En la configuración se especifica una lista separada por comas de servidores con formato de URL, nombre de host o IP. Esta configuración es válida únicamente si la opción "Tipo de conexión" no se establece en "Microsoft".
Tipo de política de enrutamiento	En la configuración se especifica el tipo de política de enrutamiento. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "Microsoft". Valores posibles: • Dividir túnel • Forzar túnel El valor predeterminado es "Forzar túnel".
Tipo de protocolo nativo	En la configuración se especifica el tipo de política de enrutamiento que utiliza la VPN. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "Microsoft". Valores posibles: • L2TP • PPTP • IKEv2 • Automático El valor predeterminado es "Automático".

Windows: configuración del perfil de VPN	Descripción
Autenticación	En la configuración se especifica el método de autenticación utilizado para la VPN nativa. La configuración "Tipo de protocolo nativo" determina qué tipos de autenticación son compatibles y el valor predeterminado de esta configuración: • Si selecciona L2TP o PPTP, los valores posibles son MS-CHAPv2 y EAP. El valor predeterminado es MS-CHAPv2. • Si selecciona IKEv2, los valores posibles son Método de usuario y Método de máquina. El valor predeterminado es Método de usuario. • Si selecciona Automático, el único valor posible es EAP. Valores posibles: • EAP • MS-CHAPv2 • Método de usuario • Método de máquina
Configuración de EAP	Este ajuste especifica el valor XML de la configuración de EAP. Para obtener información acerca de cómo generar la configuración de EAP del valor XML, visite https://docs.microsoft.com/en-us/windows/client-management/mdm/eap-configuration Esta configuración es válida únicamente si la opción "Autenticación" se establece en "EAP".
Método de usuario	En la configuración se especifica el tipo de autenticación del método de usuario que se utiliza. Esta configuración es válida únicamente si la opción "Autenticación" se establece en "Método de usuario". Valores posibles: • EAP
Método de máquina	En la configuración se especifica el tipo de autenticación del método de máquina que se utiliza. Esta configuración es válida únicamente si la opción "Autenticación" se establece en "Método de máquina". Valor posible: • Certificado
Configuración personalizada	En la configuración se especifica el Blob XML codificado en HTML para una configuración específica del complemento SSL-VPN, incluida la información de autenticación enviada al dispositivo para que esté disponible para los complementos SSL-VPN. Esta configuración es válida únicamente si la opción "Tipo de conexión" no se establece en "Microsoft".

Windows: configuración del perfil de VPN	Descripción
Nombre de la familia del paquete del complemento	En la configuración se especifica el nombre de la familia del paquete de la SSL VPN personalizada. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "Definición de conexión manual".
Clave compartida previamente de L2TP	Esta configuración especifica la clave compartida previamente que se debe utilizar para una conexión L2TP.
Lista de activadores de la aplicación	En la configuración se especifica una lista de aplicaciones que inician la conexión VPN.
Lista de activadores de la aplicación > ID de la aplicación	En la configuración se especifica una aplicación para la VPN por aplicación. Valores posibles: • Nombre de la familia del paquete. Para encontrar el nombre de la familia del paquete, instale la aplicación y ejecute el comando de Windows PowerShell, `Get-AppxPackage`. Para obtener más información, visite http://technet.microsoft.com/en-us/library/hh856044.aspx • Ubicación de la instalación de la aplicación. Por ejemplo, C:\Windows\System\Notepad.exe.
Lista de rutas	En la configuración se especifica una lista de rutas que puede utilizar la VPN. Si la VPN utiliza la tunelización dividida, se requerirá una lista de rutas.
Dirección de subred	En la configuración se especifica la dirección IP del prefijo de destino con el formato de dirección IPv4 o IPv6.
Prefijo de subred	En la configuración se especifica el prefijo de subred del prefijo de destino.
Exclusión	Esta configuración especifica si la ruta que se ha agregado debe señalar a la interfaz VPN como la puerta de enlace o a una interfaz física. Si activa la casilla de verificación, el tráfico se dirige a través de la interfaz física. Si deja la casilla desactivada, el tráfico se dirige a través de la VPN.
Lista de nombres de dominio	En la configuración se especifican las reglas de la tabla NRPT (Name Resolution Policy Table, tabla de políticas de resolución de nombres) para la VPN.
Nombre de dominio	En la configuración se especifica el FQDN o sufijo del dominio.
Servidores DNS	En la configuración se especifica la lista de direcciones IP de los servidores DNS, separadas por comas.
Servidor proxy de la web	En la configuración se especifica la dirección IP del servidor proxy de la web.
Activar VPN	Esta configuración especifica si desea que esta regla de nombre de dominio active la VPN.
Persistente	Esta configuración especifica si desea que la regla de nombre de dominio se aplique cuando la VPN no esté conectada.

Windows: configuración del perfil de VPN	Descripción
Lista de filtros de tráfico	En la configuración se especifican las reglas que permiten el tráfico a través de la VPN.
Lista de filtros de tráfico > ID de la aplicación	En la configuración se especifica una aplicación para un filtro de tráfico basado en la aplicación. Valores posibles: • Nombre de la familia del paquete. Para encontrar el nombre de la familia del paquete, instale la aplicación y ejecute el comando de Windows PowerShell, `Get-AppxPackage`. Para obtener más información, visite http://technet.microsoft.com/en-us/library/hh856044.aspx • Ubicación de la instalación de la aplicación. Por ejemplo, `C:\Windows\System\Notepad.exe`. • Escriba "SYSTEM" para que los controladores de kernel puedan enviar el tráfico a través de VPN (por ejemplo, PING o SMB).
Protocolo	En la configuración se especifica el protocolo que utiliza la VPN. Valores posibles: • Todas • TCP • UDP El valor predeterminado es "Todo".
Intervalos de puertos locales	En la configuración se especifica la lista de intervalos de puertos locales permitidos, separados por comas. Por ejemplo, 100-120, 200, 300-320.
Intervalos de puertos remotos	En la configuración se especifica la lista de intervalos de puertos remotos permitidos, separados por comas. Por ejemplo, 100-120, 200, 300-320.
Intervalos de direcciones locales	En la configuración se especifica la lista de intervalos de direcciones IP locales permitidos, separados por comas.
Intervalos de direcciones remotas	En la configuración se especifica la lista de intervalos de direcciones IP remotas permitidos, separados por comas.
Tipo de política de enrutamiento	En la configuración se especifica la política de enrutamiento que utiliza el filtro de tráfico. Si se establece en "Forzar túnel", todo el tráfico pasa a través de la VPN. Si se establece en "Dividir túnel", el tráfico puede pasar a través de la VPN o de internet. Valores posibles: • Dividir túnel • Forzar túnel La configuración predeterminada es "Forzar túnel".
Recordar credenciales	En la configuración se especifica si las credenciales se almacenan en caché siempre que sea posible.

Windows: configuración del perfil de VPN	Descripción
Siempre activado	En la configuración se especifica si los dispositivos se conectarán automáticamente a la VPN al iniciar sesión y si se mantendrán conectados hasta que el usuario desconecte manualmente la VPN.
Bloqueo	Este ajuste especifica si la conexión VPN se debe usar cuando el dispositivo se conecta a una red. Cuando esta opción está activada, se aplica lo siguiente: • El dispositivo permanece conectado a la VPN. No puede desconectarse. • El dispositivo debe estar conectado a esta red VPN para utilizar cualquier conexión de red. • El dispositivo no puede conectarse a, o modificar, otros perfiles VPN.
Sufijo DNS	En la configuración se especifican uno o varios sufijos DNS separados por comas. El primer sufijo DNS de la lista también se empleará como la conexión principal para la VPN. La lista se agrega a la lista de búsqueda de sufijos.
Detección de redes de confianza	En la configuración se especifica una cadena separada por comas para identificar las redes de confianza. La VPN no se conecta automáticamente cuando los usuarios están en la red inalámbrica de la empresa.
Propiedades de seguridad IP	
Constantes de transformación de autenticación	Valores posibles: • MD596 • SHA196 • SHA256128 • GCMAES128 • GCMAE192 • GCMAES256 La configuración predeterminada es "MD596".
Constantes de transformación de cifrado	Valores posibles: • DES • DES3 • AES128 • AES192 • AES256 • GCMAES128 • GCMAES192 • GCMAES256 La configuración predeterminada es "DES".

Windows: configuración del perfil de VPN	Descripción
Método de cifrado	Valores posibles: • DES • DES3 • AES128 • AES192 • AES256 La configuración predeterminada es "DES".
Método de comprobación de integridad	Valores posibles: • MD5 • SHA196 • SHA256 • SHA384 La configuración predeterminada es "MD5".
Grupo Diffie-Hellman	Valores posibles: • Group1 • Group2 • Group14 • ECP256 • ECP384 • Group24 La configuración predeterminada es "Group1".
Grupo PFS	Valores posibles: • PFS1 • PFS2 • PFS2048 • ECP256 • ECP384 • PFSMM • PFS24 El valor predeterminado es "PFS1".
Tipo de proxy	Esta configuración especifica el tipo de configuración de proxy para la VPN. Valores posibles: • Ninguno • Configuración de PAC • Configuración manual El valor predeterminado es "Ninguno".

Windows: configuración del perfil de VPN	Descripción
URL de PAC	En la configuración se especifica la URL del servidor web que aloja el archivo de PAC incluido el nombre del archivo. Por ejemplo, http://www.example.com/PACfile.pac. Esta configuración es válida únicamente si la opción "Tipo de proxy" se establece en "Configuración de PAC".
Dirección	En la configuración se especifican las direcciones FQDN o IP del servidor proxy. Esta configuración es válida únicamente si la opción "Tipo de proxy" se establece en "Configuración manual".
Perfil SCEP asociado	En la configuración se especifica el perfil SCEP asociado que un dispositivo debe utilizar para obtener un certificado de cliente con el objetivo de autenticarlo con la VPN .

Ajustes del perfil SCEP

Puede utilizar una variable en cualquier ajuste de perfil que sea un campo de texto para hacer referencia a un valor en lugar de especificar el valor real. BlackBerry UEM admite variables predeterminadas que son variables predefinidas y personalizadas que se definen. Los perfiles SCEP son compatibles con los siguientes tipos de dispositivos:

- BlackBerry 10
- iOS
- macOS
- Android
- Windows 10

En algunos casos, la versión mínima del SO del dispositivo requerida para que sea compatible con una configuración es una versión no admitida por BlackBerry UEM. Para obtener más información acerca de las versiones OS compatibles, consulte la Matriz de compatibilidad.

Común: ajustes del perfil SCEP

Común: configuración del perfil SCEP	Descripción
Conexión con la autoridad de certificación	Esta configuración especifica si la CA es Entrust, OpenTrust u otra CA. Si ha configurado una o más conexiones al software Entrust o OpenTrust de la empresa, puede seleccionar una de las conexiones en la lista desplegable. Seleccione Genérico si está usando cualquier otra CA. Si selecciona una conexión Entrust o OpenTrust, a continuación debe seleccionar el perfil de PKI adecuado y especificar los valores necesarios. Los perfiles disponibles varían en función de lo que el administrador de Entrust o OpenTrust haya configurado en el software de PKI. El valor predeterminado es Genérico.

Común: configuración del perfil SCEP	Descripción
URL	Este ajuste especifica la URL del servicio SCEP. La URL debe incluir el protocolo, el FQDN, el número de puerto y la ruta SCEP (la ruta CGI que se define en la especificación SCEP). Debe establecer un valor la configuración para activar un dispositivo correctamente. Las URL HTTPS SCEP son compatibles con los dispositivos iOS y la versión BlackBerry 10 OS 10.3.0 o posterior.
Nombre de la instancia	Este ajuste especifica el nombre de la instancia de la autoridad de certificación. El valor puede ser cualquier cadena que sea entendida por el servicio SCEP. Por ejemplo, podría tratarse de un nombre de dominio como example.org. Si una CA tiene varios certificados de CA, este campo puede utilizarse para distinguir cuál se necesita.
Tipo de desafío SCEP	En la configuración se especifica si la contraseña de comprobación SCEP se genera dinámicamente o como una contraseña estática. Si la configuración se establece en "Estático", todos los dispositivos utilizarán la misma contraseña de comprobación. Si la configuración se establece en "Dinámico", cada dispositivo recibirá una contraseña de comprobación exclusiva. Valores posibles: • Estático • Dinámico El valor predeterminado es Dinámico. Para los dispositivos Windows, únicamente se admiten contraseñas "Estáticas".
URL de generación de contraseñas de comprobación	En la configuración se especifica la URL que el dispositivo utiliza para obtener una contraseña de comprobación generada dinámicamente desde el servicio SCEP. La URL debe incluir el protocolo, el dominio, el puerto y la ruta SCEP (la ruta CGI que se define en la especificación SCEP). Si utiliza una contraseña de comprobación dinámica, debe establecer un valor para activar los dispositivos BlackBerry 10 correctamente. Esta configuración es válida únicamente si la opción "Tipo de desafío SCEP" se establece en "Dinámico".
Tipo de autenticación	En la configuración se especifica el tipo de autenticación que los dispositivos utilizan para conectarse al servicio SCEP y obtener una contraseña de comprobación. Esta configuración es válida únicamente si la opción "Tipo de desafío SCEP" se establece en "Dinámico". Valores posibles: • Básico • NTLM El valor predeterminado es Básico.

Común: configuración del perfil SCEP	Descripción
Dominio	En la configuración se especifica el dominio utilizado para la autenticación NTLM cuando los dispositivos se conectan al servicio SCEP para obtener una contraseña de comprobación. Esta configuración es válida únicamente si la opción "Tipo de autenticación" se establece en "NTLM".
Nombre de usuario	La contraseña especifica el nombre de usuario requerido para obtener una contraseña de comprobación desde el servicio SCEP. Esta configuración es válida únicamente si la opción "Tipo de desafío SCEP" se establece en "Dinámico".
Contraseña	La contraseña especifica la contraseña requerida para obtener la contraseña de comprobación desde el servicio SCEP. Esta configuración es válida únicamente si la opción "Tipo de desafío SCEP" se establece en "Dinámico".
Contraseña de comprobación	Esta configuración especifica la contraseña de comprobación que un dispositivo utiliza para la inscripción de certificados. Si utiliza una contraseña de comprobación estática, debe establecer un valor para la configuración a fin de activar los dispositivos BlackBerry 10 correctamente. Esta configuración es válida únicamente si la opción "Tipo de desafío SCEP" se establece en "Estático".

BlackBerry 10: ajustes del perfil SCEP

BlackBerry 10: configuración del perfil SCEP	Descripción
Usar asunto predeterminado y nombre alternativo del asunto del dispositivo	En la configuración se especifica si un dispositivo BlackBerry 10 genera el asunto y el nombre alternativo del asunto para una solicitud de certificado. Si no se selecciona este ajuste, deberá especificar el asunto y el tipo y el valor del nombre alternativo del asunto.
Asunto	En la configuración se especifica el asunto del certificado si es necesario para la configuración SCEP de la empresa. Escriba el asunto en el formato "/CN=<*common_name*>/O=<*domain_name*>". Si el perfil es para varios usuarios, puede utilizar una variable, por ejemplo: %UserDistinguishedName%. Esta configuración es válida únicamente si se ha seleccionado la opción "Usar asunto predeterminado y nombre alternativo del asunto del dispositivo". El requisito mínimo es BlackBerry 10 OS versión 10.3.1.

BlackBerry 10: configuración del perfil SCEP	Descripción
SAN	En la configuración se especifica el tipo y el valor del nombre alternativo del asunto para un certificado. Esta configuración es válida únicamente si se ha seleccionado la opción "Usar asunto predeterminado y nombre alternativo del asunto del dispositivo". El requisito mínimo es BlackBerry 10 OS versión 10.3.1.
Tipo de SAN	En la configuración se especifica el tipo de nombre alternativo del asunto del certificado, si es necesario. Valores posibles: • Nombre de RFC 822 • URI • Nombre principal de NT • Nombre de DNS El valor predeterminado es "Nombre de RFC 822".
Valor de SAN	En la configuración se especifica la representación alternativa del asunto del certificado. El valor debe ser una dirección de correo, el nombre DNS del servidor CA, la URL completa del servidor o el nombre principal. El ajuste "Tipo de SAN" determina el valor adecuado que se debe especificar. Si se establece en "Nombre de RFC822" el valor debe ser una dirección de correo válida. Si se establece en "URI", el valor debe ser una URL válida que incluya el protocolo y la dirección IP o FQDN. Si se establece en "Nombre principal de NT", el valor debe ser un nombre principal válido. Si se establece en "Nombre de DNS", el valor debe ser un FQDN válido.
Algoritmo de clave	Esta configuración especifica el algoritmo que un dispositivo BlackBerry 10 debe utilizar para generar el par de claves del cliente. Debe seleccionar un algoritmo que sea compatible con su CA. Valores posibles: • Ninguna • RSA • ECC El valor predeterminado es "RSA ".

BlackBerry 10: configuración del perfil SCEP	Descripción
Intensidad de RSA	Esta configuración especifica la intensidad de RSA que un dispositivo BlackBerry 10 debe utilizar para generar el par de claves del cliente. Debe introducir una intensidad de la clave que sea compatible con su CA. Esta configuración es válida únicamente si la opción "Algoritmo de clave" se establece en "RSA ". Valores posibles: • 1024 • 2048 • 4096 • 8192 • 16384 El valor predeterminado es "1024".
Intensidad de ECC	Esta configuración especifica la curva elíptica que un dispositivo BlackBerry 10 debe utilizar para generar el par de claves del cliente. La curva elíptica define la intensidad del par de claves del cliente. Debe seleccionar una curva elíptica que sea compatible con su CA. Esta configuración es válida únicamente si la opción "Algoritmo de clave" se establece en "ECC". Valores posibles: • sect163k1 • sect283k1 • secp192r1 • secp256r1 • secp384r1 • secp521r1 El valor predeterminado es "secp521r1".
Algoritmo de cifrado	Esta configuración especifica el algoritmo de cifrado que un dispositivo BlackBerry 10 utiliza para la solicitud de inscripción de certificados. Valores posibles: • Ninguna • Triple DES • AES (128 bits) • AES (196 bits) • AES (256 bits) El valor predeterminado es "Triple DES".

BlackBerry 10: configuración del perfil SCEP	Descripción
Función hash	Esta configuración especifica la función hash que un dispositivo BlackBerry 10 utiliza para la solicitud de inscripción de certificados. Valores posibles: • Ninguna • SHA-1 • SHA-224 • SHA-256 • SHA-384 • SHA-512 El valor predeterminado es "SHA-1".
Huella digital de certificado	En la configuración se especifica el hash de cifrado hexadecimal del certificado raíz para la autoridad de certificación. Puede utilizar los siguientes algoritmos para especificar la huella digital: MD5, SHA-1, SHA-224, SHA-256, SHA-384 y SHA-512. Debe establecer un valor para esta configuración para que se active correctamente un dispositivo BlackBerry 10.
Renovación automática	En la configuración se especifica con cuántos días de antelación se realiza la renovación automática antes de que el certificado caduque. Los valores posibles son de 1 a 999 999 999 días. El valor predeterminado es "30".
Uso de la clave	En la configuración se especifican las operaciones criptográficas que se pueden realizar con la clave pública incluida en el certificado. Selecciones posibles: • Firma digital • Sin rechazo • Cifrado de clave • Cifrado de datos • Acuerdo de clave • Firma del certificado de clave • Firma de CRL • Solo cifrado • Solo descifrado Las selecciones predeterminadas son "Firma digital", "Cifrado de clave" y "Acuerdo de clave". El requisito mínimo es BlackBerry 10 OS versión 10.3.1.

BlackBerry 10: configuración del perfil SCEP	Descripción
Uso extendido de la clave	En la configuración se especifica la finalidad de la clave contenida en el certificado. Selecciones posibles: • Autenticación de servidor • Autenticación de cliente • Firma de código • Protección de correo • Marca de hora • Firma de OCSP • Cliente de shell seguro • Servidor de shell seguro La selección predeterminada es "Autenticación de cliente". El requisito mínimo es BlackBerry 10 OS versión 10.3.1.

iOS: ajustes del perfil SCEP

iOS: configuración del perfil SCEP	Descripción
Usar BlackBerry UEM como proxy para solicitudes SCEP	En la configuración se especifica si todas las solicitudes SCEP desde los dispositivos se envían a través de BlackBerry UEM. Si la CA está detrás del firewall, la configuración permitirá inscribir certificados de cliente en los dispositivos sin exponer la CA fuera del firewall.
Asunto	En la configuración se especifica el asunto del certificado si es necesario para la configuración SCEP de la empresa. Escriba el asunto en el formato "/CN=<*common_name*>/O=<*domain_name*>". Si el perfil es para varios usuarios, puede utilizar una variable, por ejemplo: %UserDistinguishedName%.
Reintentos	En la configuración se especifica cuántas veces debe volver a intentarse la conexión al servicio SCEP si el intento de conexión falla. Los valores posibles son de 1 a 999. El valor predeterminado es "3".
Intervalo entre reintentos	En la configuración se especifica el tiempo en segundos que hay que esperar antes de intentar conectarse al servicio SCEP. Los valores posibles son de 1 a 999. El valor predeterminado es "10" segundos.

iOS: configuración del perfil SCEP	Descripción
Tamaño de clave	Esta configuración especifica el tamaño de clave para el certificado. Valores posibles: • 1024 • 2048 El valor predeterminado es 1024.
Huella dactilar	En la configuración se especifica la huella digital para inscribir un certificado SCEP. Si la CA utiliza HTTP en lugar de HTTPS, los dispositivos utilizan la huella digital para confirmar la identidad de la CA durante el proceso de inscripción. La huella dactilar no puede contener espacios.
Tipo de SAN	En la configuración se especifica el tipo de nombre alternativo del asunto del certificado, si es necesario. Valores posibles: • Ninguna • Nombre de RFC822 • Nombre de DNS • Uniform Resource Identifier (Identificador de recursos uniforme) El valor predeterminado es "Ninguno".
Valor de SAN	En la configuración se especifica la representación alternativa del asunto del certificado. El valor debe ser una dirección de correo, el nombre DNS del servidor CA, la URL completa del servidor. El ajuste "Tipo de SAN" determina el valor adecuado que se debe especificar. Si se establece en "Nombre de RFC822" el valor debe ser una dirección de correo válida. Si se establece en "URI", el valor debe ser una URL válida que incluya el protocolo y la dirección IP o FQDN. Si se establece en "Nombre principal de NT", el valor debe ser un nombre principal válido. Si se establece en "Nombre de DNS", el valor debe ser un FQDN válido.
Nombre principal de NT	En la configuración se especifica el nombre principal de NT para la generación del certificado. Esta configuración es válida únicamente si la opción "Tipo de SAN" se establece en un valor distinto de "Ninguno".
Caducidad del perfil	Especifique el número de días después de la emisión del certificado en el que el dispositivo solicita un nuevo certificado de la CA. Si el certificado del dispositivo se ha emitido antes de actualizar a BlackBerry UEM versión 12.8, la primera solicitud de renovación se producirá después del número especificado de días tras la actualización de UEM. El valor debe ser inferior al periodo de validez del certificado definido por la CA. El valor máximo es 1825 días.

macOS: ajustes del perfil de SCEP

macOS aplica perfiles a las cuentas de usuario o los dispositivos. Puede configurar perfiles SCEP para aplicarlos a uno u otro.

macOS: configuración del perfil SCEP	Descripción
Usar BlackBerry UEM como proxy para solicitudes SCEP	En la configuración se especifica si todas las solicitudes SCEP desde los dispositivos se envían a través de BlackBerry UEM. Si la CA está detrás del firewall, la configuración permitirá inscribir certificados de cliente en los dispositivos sin exponer la CA fuera del firewall.
Aplicar perfil a	En la configuración se especifica si el perfil SCEP se aplica a la cuenta de usuario o al dispositivo. Valores posibles: • Usuario • Dispositivo
Asunto	En la configuración se especifica el asunto del certificado si es necesario para la configuración SCEP de la empresa. Escriba el asunto en el formato "/CN=<*common_name*>/O=<*domain_name*>". Si el perfil es para varios usuarios, puede utilizar una variable, por ejemplo: %UserDistinguishedName%.
Reintentos	En la configuración se especifica cuántas veces debe volver a intentarse la conexión al servicio SCEP si el intento de conexión falla. Los valores posibles son de 1 a 999. El valor predeterminado es "3".
Intervalo entre reintentos	En la configuración se especifica el tiempo en segundos que hay que esperar antes de intentar conectarse al servicio SCEP. Los valores posibles son de 1 a 999. El valor predeterminado es "10" segundos.
Tamaño de clave	Esta configuración especifica el tamaño de clave para el certificado. Valores posibles: • 1024 • 2048 El valor predeterminado es "1024".
Huella dactilar	En la configuración se especifica la huella digital para inscribir un certificado SCEP. Si la CA utiliza HTTP en lugar de HTTPS, los dispositivos utilizan la huella digital para confirmar la identidad de la CA durante el proceso de inscripción. La huella dactilar no puede contener espacios.

macOS: configuración del perfil SCEP	Descripción
Tipo de SAN	En la configuración se especifica el tipo de nombre alternativo del asunto del certificado, si es necesario. Valores posibles: • Ninguna • Nombre de RFC822 • Nombre de DNS • Uniform Resource Identifier (Identificador de recursos uniforme) El valor predeterminado es "Ninguno".
Valor de SAN	En la configuración se especifica la representación alternativa del asunto del certificado. El valor debe ser una dirección de correo, el nombre DNS del servidor CA, la URL completa del servidor. El ajuste "Tipo de SAN" determina el valor adecuado que se debe especificar. Si se establece en "Nombre de RFC822" el valor debe ser una dirección de correo válida. Si se establece en "URI", el valor debe ser una URL válida que incluya el protocolo y la dirección IP o FQDN. Si se establece en "Nombre principal de NT", el valor debe ser un nombre principal válido. Si se establece en "Nombre de DNS", el valor debe ser un FQDN válido.
Nombre principal de NT	En la configuración se especifica el nombre principal de NT para la generación del certificado. Esta configuración es válida únicamente si la opción "Tipo de SAN" se establece en un valor distinto de "Ninguno".

Android: ajustes del perfil SCEP

Para ver un ejemplo de un perfil SCEP para dispositivos Android, visite http://support.blackberry.com/kb/ para leer el artículo KB38248.

Android: configuración del perfil SCEP	Descripción
Usar BlackBerry UEM como proxy para solicitudes SCEP	En la configuración se especifica si todas las solicitudes SCEP desde los dispositivos se envían a través de BlackBerry UEM. Si la CA está detrás del firewall, la configuración permitirá inscribir certificados de cliente en los dispositivos sin exponer la CA fuera del firewall.

Android: configuración del perfil SCEP	Descripción
Algoritmo de cifrado	Esta configuración especifica el algoritmo de cifrado que un dispositivo Android utiliza para la solicitud de inscripción de certificados. Valores posibles: • Ninguna • Triple DES • AES (128 bits) • AES (196 bits) • AES (256 bits) El valor predeterminado es "Triple DES".
Función hash	Esta configuración especifica la función hash que un dispositivo Android utiliza para la solicitud de inscripción de certificados. Valores posibles: • Ninguna • SHA-1 • SHA-224 • SHA-256 • SHA-384 • SHA-512 El valor predeterminado es "SHA-1".
Huella digital de certificado	En la configuración se especifica el hash de cifrado hexadecimal del certificado raíz para la autoridad de certificación. Puede utilizar los siguientes algoritmos para especificar la huella digital: SHA-1, SHA-224, SHA-256, SHA-384 y SHA-512. Debe establecer un valor para esta configuración si quiere activar dispositivos que utilicen perfiles de trabajo de Android o Samsung KNOX.
Renovación automática	En la configuración se especifica con cuántos días de antelación se realiza la renovación automática antes de que el certificado caduque. Los valores posibles son de 1 a 365. El valor predeterminado es "30".
Android work profiles / Samsung KNOX	
Asunto	En la configuración se especifica el asunto del certificado si es necesario para la configuración SCEP de la empresa. Escriba el asunto en el formato "/CN=<*common_name*>/O=<*domain_name*>". Si el perfil es para varios usuarios, puede utilizar una variable, por ejemplo: %UserDistinguishedName%.

Android: configuración del perfil SCEP	Descripción
Tipo de SAN	En la configuración se especifica el tipo de nombre alternativo del asunto del certificado, si es necesario. Valores posibles: • Nombre de RFC 822 • Identificador uniforme de recursos • Nombre principal de NT • Nombre de DNS El valor predeterminado es "Nombre de RFC 822".
Valor de SAN	En la configuración se especifica la representación alternativa del asunto del certificado. El valor debe ser una dirección de correo, el nombre DNS del servidor CA, la URL completa del servidor o el nombre principal. El ajuste "Tipo de SAN" determina el valor adecuado que se debe especificar. Si se establece en "Nombre de RFC822" el valor debe ser una dirección de correo válida. Si se establece en "URI", el valor debe ser una URL válida que incluya el protocolo y la dirección IP o FQDN. Si se establece en "Nombre principal de NT", el valor debe ser un nombre principal válido. Si se establece en "Nombre de DNS", el valor debe ser un FQDN válido.
Algoritmo de clave	Esta configuración especifica el algoritmo que los dispositivos con perfiles de trabajo de Android o Samsung KNOX deben utilizar para generar el par de claves del cliente. Debe seleccionar un algoritmo que sea compatible con su CA. Valores posibles: • Ninguna • RSA • ECC El valor predeterminado es "RSA ".
Intensidad de RSA	Esta configuración especifica la potencia RSA que los dispositivos con perfiles de trabajo de Android o Samsung KNOX deben utilizar para generar el par de claves del cliente. Debe introducir una intensidad de la clave que sea compatible con su CA. Esta configuración solo es válida si la opción "Algoritmo de clave" se establece en "RSA ". Valores posibles: • 1024 • 2048 • 4096 • 8192 • 16384 El valor predeterminado es "1024".

Android: configuración del perfil SCEP	Descripción
Uso de la clave	En la configuración se especifican las operaciones criptográficas que se pueden realizar con la clave pública que está incluida en el certificado. Selecciones posibles: • Firma digital • Sin rechazo • Cifrado de clave • Cifrado de datos • Acuerdo de clave • Firma del certificado de clave • Firma de CRL • Solo cifrado • Solo descifrado Las selecciones predeterminadas son "Firma digital", "Cifrado de clave" y "Acuerdo de clave".
Uso extendido de la clave	En la configuración se especifica la finalidad de la clave que está incluida en el certificado. Selecciones posibles: • Autenticación de servidor • Autenticación de cliente • Firma de código • Protección de correo • Marca de hora • Firma de OCSP • Cliente de shell seguro • Servidor de shell seguro La selección predeterminada es "Autenticación de cliente".

Windows 10: ajustes del perfil SCEP

Windows 10: configuración del perfil SCEP	Descripción
Asunto	En la configuración se especifica el asunto del certificado si es necesario para la configuración SCEP de la empresa. Escriba el asunto en el formato "/CN=<*common_name*>/O=<*domain_name*>". Si el perfil es para varios usuarios, puede utilizar una variable, por ejemplo: %UserDistinguishedName%.

Windows 10: configuración del perfil SCEP	Descripción
Tipo de SAN	En la configuración se especifica el tipo de nombre alternativo del asunto del certificado, si es necesario. Valores posibles: • Ninguna • Nombre de RFC 822 • Nombre de DNS • Identificador uniforme de recursos El valor predeterminado es "Ninguno".
Valor de SAN	En la configuración se especifica la representación alternativa del asunto del certificado. El valor debe ser una dirección de correo, el nombre DNS del servidor CA, la URL completa del servidor. El valor apropiado para este ajuste dependerá del valor seleccionado para el ajuste "Tipo de SAN".
Reintentos	En la configuración se especifica cuántas veces debe volver a intentarse la conexión al servicio SCEP si el intento de conexión falla. Los valores posibles son de 1 a 999. El valor predeterminado es "3".
Intervalo entre reintentos	En la configuración se especifica el tiempo en segundos que hay que esperar antes de intentar conectarse al servicio SCEP. Los valores posibles son de 1 a 999. El valor predeterminado es "10" segundos.
Tamaño de clave	Esta configuración especifica el tamaño de clave para el certificado. Valores posibles: • 1024 • 2048 • 4096 • 8192 • 16384 El valor predeterminado es "1024".

Windows 10: configuración del perfil SCEP	Descripción
Uso de la clave	En la configuración se especifican las operaciones criptográficas que se pueden realizar con la clave pública que está incluida en el certificado. • Firma digital • Sin rechazo • Cifrado de clave • Cifrado de datos • Acuerdo de clave • Firma del certificado de clave • Firma de CRL • Solo cifrado Las selecciones predeterminadas son "Firma digital", "Cifrado de clave" y "Acuerdo de clave".
Uso extendido de la clave	En la configuración se especifica la finalidad de la clave que está incluida en el certificado. • Autenticación de servidor • Autenticación de cliente • Firma de código • Protección de correo • Marca de hora • Firma de OCSP • Cliente de shell seguro • Servidor de shell seguro La selección predeterminada es "Autenticación de cliente".
Función hash	Esta configuración especifica la función hash que un dispositivo Windows 10 utiliza para la solicitud de inscripción de certificados. Valores posibles: • SHA-1 • SHA-224 • SHA-256 • SHA-384 • SHA-512 El valor predeterminado es "SHA-1".
Huella digital de certificado	En la configuración se especifica el hash de cifrado hexadecimal del certificado raíz para la autoridad de certificación. Puede utilizar los siguientes algoritmos para especificar la huella digital: SHA-1, SHA-224, SHA-256, SHA-384 y SHA-512.

Windows 10: configuración del perfil SCEP	Descripción
Renovación automática	En la configuración se especifica con cuántos días de antelación se realiza la renovación automática antes de que el certificado caduque. Los valores posibles son de 1 a 365. El valor predeterminado es "30".

BlackBerry Dynamics: SCEP profile settings

These settings apply to SCEP certificates used with BlackBerry Dynamics apps on iOS and Android devices.

BlackBerry Dynamics: SCEP profile setting	Description
Subject	This setting specifies the subject for the certificate, if required for your organization's SCEP configuration. Type the subject in the format "/CN=<*common_name*>,O=<*domain_name*>" If the profile is for multiple users, you can use a variable, for example: %UserDistinguishedName%.
SAN type	This setting specifies the subject alternative name type for the certificate, if it is required. Possible values: • RFC 822 name • Uniform resource identifier • NT principal name • DNS name The default value is "RFC 822 name."
SAN value	This setting specifies the subject alternative representation of the certificate subject. The value must be an email address, the DNS name of the CA server, the fully qualified URL of the server, or principal name. The "SAN type" setting determines the appropriate value to specify. If set to "RFC822 name," the value must be a valid email address. If set to "URI," the value must be a valid URL that includes the protocol and FQDN or IP address. If set to "NT principal name," the value must be a valid principal name. If set to "DNS name," the value must be a valid FQDN.
Key algorithm	This setting specifies the algorithm used to generate the client key pair. You must select an algorithm that is supported by your CA. Possible values: • RSA

BlackBerry Dynamics: SCEP profile setting	Description
RSA strength	This setting specifies the RSA strength used to generate the client key pair. You must enter a key strength that is supported by your CA. This setting is valid only if the "Key algorithm" setting is set to "RSA.". Possible values: • 2048 • 4096 The default value is "2048."
Encryption algorithm	This setting specifies the encryption algorithm used for the certificate enrollment request. Possible values: • Triple DES • AES (128-bit) • AES (196-bit) • AES (256-bit) The default value is "Triple DES."
Hash function	This setting specifies the hash function used for the certificate enrollment request. Possible values: • SHA-256 • SHA-384 • SHA-512 The default value is "SHA-256."
Certificate thumbprint	This setting specifies the hexadecimal-encoded hash of the root certificate for the CA. You can use one of the following algorithms to specify the thumbprint: SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512. MD5 is supported only if "Enable FIPS" is not selected in the BlackBerry Dynamics profile.
Automatic renewal	This setting specifies how many days before a certificate expires that automatic certificate renewal occurs. The possible values are 1 to 365. The default value is "30."

BlackBerry Dynamics: SCEP profile setting	Description
Key usage	This setting specifies the cryptographic operations that can be performed using the public key that is contained in the certificate. Possible selections: • Digital signature • Non-repudiation • Key encipherment • Data encipherment • Key agreement • Key certificate signing • CRL signing • Encipher only • Decipher only The default selections are "Digital signature," "Key encipherment," and "Key agreement."
Extended key usage	This setting specifies the purpose of the key that is contained in the certificate. Possible selections: • Server authentication • Client authentication • Code signing • Email protection • Time stamping • OCSP signing • Secure shell client • Secure shell server The default selection is "Client authentication."
App restrictions	This setting specifies which BlackBerry Dynamics apps can use the certificate. Possible values: • Allow all apps to use certificates • Allow specified apps to use certificates The default selection is "Allow all apps to use certificates."
Apps allowed to use SCEP	This setting specifies which apps are allowed to use SCEP certificates. This setting is valid only if the "App restrictions" setting is set to "Allow specified apps to use certificates."
Delete expired certificates	This setting specifies whether the device deletes expired certificates.
Remove duplicate certificates	This setting specifies whether the device deleted duplicate certificates. The device deletes the certificate that has the earliest start date.

Configuración del perfil de conformidad

Los perfiles de conformidad son compatibles con los siguientes tipos de dispositivos:

- BlackBerry 10
- iOS
- macOS
- Android
- Windows

Común: configuración del perfil de conformidad

Para cada regla de conformidad que seleccione en las pestañas del dispositivo, elija la acción que desea que BlackBerry UEM realice si un dispositivo del usuario no cumple los requisitos.

Común: configuración del perfil de conformidad	Descripción
Acción de cumplimiento	Esta configuración especifica la acción que BlackBerry UEM realiza en dispositivos que no cumplen los requisitos. Valores posibles: • Aviso sobre conformidad • No es de confianza: en dispositivos iOS, macOS, Android y Windows, esta opción evita que el usuario acceda a aplicaciones y recursos de trabajo desde el dispositivo. Los datos y las aplicaciones no se eliminan del dispositivo. **Nota:** Untrust no es compatible con las aplicaciones de BlackBerry Dynamics. **Nota:** En dispositivos iOS, la cuenta de correo de trabajo se elimina de la aplicación de correo nativa. Los usuarios deben restaurar la configuración de la cuenta de correo en la aplicación después de que el dispositivo vuelva a cumplir los requisitos. • Cuarentena: en dispositivos con BlackBerry 10, esta opción evita que el usuario acceda a los recursos y aplicaciones de trabajo desde el dispositivo. Los datos y las aplicaciones no se eliminan del dispositivo. • Eliminar solo los datos de trabajo • Eliminar todos los datos • Eliminar del servidor: en los dispositivos con BlackBerry 10, iOS,Android y Windows, se puede desactivar un dispositivo de BlackBerry UEM si infringe la regla "Fuera de contacto". • Ninguno: permite identificar una infracción de la conformidad, pero no se realiza ninguna acción. El valor predeterminado es "Aviso sobre conformidad". En los dispositivos activados con "Trabajo y personal: privacidad de usuario", no puede eliminar todos los datos del dispositivo del usuario. Si selecciona "Eliminar todos los datos", BlackBerry UEM realiza la misma acción que "Eliminar solo los datos de trabajo". Para los dispositivos Samsung KNOX Workspace que solo cuentan con un espacio de trabajo, si selecciona "Eliminar solo los datos de trabajo", "Eliminar todos los datos" o "Eliminar del servidor", se eliminarán todos los datos del dispositivo. Para dispositivos supervisados con iOS 9.3.2 y posterior, las acciones de cumplimiento para la regla "La aplicación restringida está instalada" no son aplicables. Se impide automáticamente que los usuarios instalen aplicaciones restringidas.

Común: configuración del perfil de conformidad	Descripción
Método de aviso	Los valores posibles son: • Ambas • Notificación de correo electrónico • Notificación del dispositivo El valor predeterminado es "Ambas". Esta configuración solo es válida si "Acción de cumplimiento" está establecida en "Aviso sobre conformidad". Los dispositivos Windows 10 no son compatibles con las notificaciones de dispositivos.
Recuento de avisos	El número de veces que se solicita al usuario que corrija la infracción. El valor predeterminado es "3". Esta configuración solo es válida si "Acción de cumplimiento" está establecida en "Aviso sobre conformidad".
Intervalo de aviso	La cantidad de tiempo entre avisos, en minutos, horas o días. El valor predeterminado es "4 horas". Esta configuración solo es válida si "Acción de cumplimiento" está establecida en "Aviso sobre conformidad".
Acción al caducar el intervalo de aviso	Esta configuración define lo que sucede cuando el usuario ha recibido el número total de avisos, tal como se define en Recuento de avisos, y no corrige la infracción. Valores posibles: • Ninguno • No es de confianza: en dispositivos iOS, macOS, Android y Windows, esta opción evita que el usuario acceda a aplicaciones y recursos de trabajo desde el dispositivo. Los datos y las aplicaciones no se eliminan del dispositivo. **Nota:** Untrust no es compatible con las aplicaciones de BlackBerry Dynamics. Utilice una acción de cumplimiento alternativa. • Cuarentena: en dispositivos con BlackBerry 10, esta opción evita que el usuario acceda a los recursos y aplicaciones de trabajo desde el dispositivo. Los datos y las aplicaciones no se eliminan del dispositivo. • Eliminar solo los datos de trabajo • Eliminar todos los datos El valor predeterminado es "No es de confianza". Esta configuración solo es válida si "Acción de cumplimiento" está establecida en "Aviso sobre conformidad".

Común: configuración del perfil de conformidad	Descripción
Acción de cumplimiento para las aplicaciones de BlackBerry Dynamics	Esta configuración define lo que ocurre con las aplicaciones de BlackBerry Dynamics cuando un dispositivo no está en conformidad. Valores posibles: • Eliminar datos de aplicaciones de BlackBerry Dynamics • No permitir la ejecución de aplicaciones de BlackBerry Dynamics El valor predeterminado es "Eliminar datos de aplicaciones de BlackBerry Dynamics".

BlackBerry 10: configuración del perfil de conformidad

Consulte Común: configuración del perfil de conformidad para obtener una explicación sobre las acciones posibles si se selecciona una regla de conformidad.

BlackBerry 10: configuración del perfil de conformidad	Descripción
Alerta de integridad	Esta configuración crea una regla de conformidad si un atacante descubre cómo obtener acceso de raíz o escalar privilegios en un dispositivo con BlackBerry 10.
Versión restringida de software instalada	Esta configuración crea una regla de conformidad para garantizar que los dispositivos no utilicen una versión restringida del software según se especifica en el perfil de requisitos de solicitud de servicio del dispositivo. Para obtener más información, consulte Crear un perfil de requisitos de solicitud de servicio del dispositivo para dispositivos con BlackBerry 10. Esta regla no se aplica a los dispositivos con el tipo de activación Trabajo y personal - Empresa.
Versión de SO restringida instalada	Esta configuración crea una regla de conformidad para garantizar que los dispositivos no tienen una versión del SO restringida instalada según se especifica en esta configuración. Puede especificar las versiones del SO restringidas.
Modelo de dispositivo restringido detectado	Esta configuración crea una regla de conformidad para restringir modelos de dispositivo según se especifica en esta configuración. Valores posibles: • Permitir modelos de dispositivo seleccionados • No permitir modelos de dispositivo seleccionados Puede seleccionar los modelos de los dispositivos que están permitidos o restringidos.
Dispositivo fuera de contacto	Esta configuración crea una regla de conformidad para garantizar que los dispositivos no están fuera de contacto con BlackBerry UEM durante más de un periodo especificado.

BlackBerry 10: configuración del perfil de conformidad	Descripción
Última hora de contacto	Esta configuración especifica el número de días que un dispositivo puede estar fuera de contacto con BlackBerry UEM. Esta configuración es válida únicamente si se ha seleccionado la opción "Dispositivo fuera de contacto".

iOS: configuración del perfil de conformidad

Consulte Común: configuración del perfil de conformidad para obtener una explicación sobre las acciones posibles si se selecciona una regla de conformidad.

iOS: configuración del perfil de conformidad	Descripción
SO liberado	Esta configuración crea una regla de conformidad para garantizar que los dispositivos iOS no se liberen. Un dispositivo se libera cuando un usuario o un atacante evitan diversas restricciones en un dispositivo para modificar el sistema operativo.
La aplicación no asignada está instalada	Esta configuración crea una regla de conformidad para garantizar que los dispositivos no tienen aplicaciones instaladas que no se asignaron al usuario. Cuando selecciona esta configuración y una aplicación no asignada está instalada en un dispositivo iOS, se muestran un mensaje de advertencia y un enlace en la pestaña Dispositivos gestionados. Al hacer clic en el enlace, se muestra una lista de las aplicaciones que hacen que el dispositivo no cumpla los requisitos de conformidad. Esta configuración no es válida para los dispositivos activados con el tipo de activación Privacidad del usuario.
La aplicación obligatoria no está instalada	Esta configuración crea una regla de conformidad para garantizar que los dispositivos tienen las aplicaciones necesarias instaladas. Cuando selecciona esta configuración y una aplicación obligatoria no está instalada en un dispositivo iOS, se muestran un mensaje de advertencia y un enlace en la pestaña Dispositivos gestionados. Al hacer clic en el enlace, se muestra una lista de las aplicaciones que hacen que el dispositivo no cumpla los requisitos de conformidad.
Versión de SO restringida instalada	Esta configuración crea una regla de conformidad para garantizar que los dispositivos no tienen una versión del SO restringida instalada según se especifica en esta configuración. Puede seleccionar las versiones del SO restringidas.

iOS: configuración del perfil de conformidad	Descripción
Modelo de dispositivo restringido detectado	Esta configuración crea una regla de conformidad para restringir modelos de dispositivo según se especifica en esta configuración. Valores posibles: • Permitir modelos de dispositivo seleccionados • No permitir modelos de dispositivo seleccionados Puede seleccionar los modelos de los dispositivos que están permitidos o restringidos.
Dispositivo fuera de contacto	Esta configuración crea una regla de conformidad para garantizar que los dispositivos no están fuera de contacto con BlackBerry UEM durante más de un periodo especificado.
Última hora de contacto	Esta configuración especifica el número de días que un dispositivo puede estar fuera de contacto con BlackBerry UEM. Esta configuración es válida únicamente si se ha seleccionado la opción "Dispositivo fuera de contacto".
Verificación de versiones de bibliotecas de BlackBerry Dynamics	Esta configuración crea una regla de conformidad que le permite seleccionar las versiones de bibliotecas de BlackBerry Dynamics que no se pueden activar. Puede seleccionar las versiones de bibliotecas bloqueadas.
Verificación de la conectividad de BlackBerry Dynamics	Esta configuración crea una regla de conformidad para garantizar que las aplicaciones de BlackBerry Dynamics no están fuera de contacto con BlackBerry UEM durante más de un periodo especificado. La acción de cumplimiento se aplica a las aplicaciones de BlackBerry Dynamics.
Basar intervalo de conectividad en las aplicaciones delegadas de la autenticación	Esta configuración especifica que la verificación de la conectividad se base en cuándo una aplicación delegada de autenticación se conecta a BlackBerry UEM. Esta configuración es válida únicamente si se ha seleccionado la opción "Verificación de la conectividad".

iOS: configuración del perfil de conformidad	Descripción
Última hora de contacto	Esta opción especifica el número de días para que el dispositivo deba conectarse a BlackBerry UEM. Valores posibles: • 8 horas • 16 horas • 1 día • 2 días • 3 días • 7 días • 14 días • 30 días • 60 días • 90 días • 180 días • 365 días El valor predeterminado es "2 días". Esta configuración es válida únicamente si se ha seleccionado la opción "Verificación de la conectividad".

iOS: configuración del perfil de conformidad	Descripción

La aplicación restringida está instalada	Esta configuración crea una regla de conformidad para impedir que los usuarios instalen aplicaciones específicas.
	
	Para restringir las aplicaciones, realice cualquiera de las siguientes tareas:
	
	• Seleccione una aplicación de la lista de aplicaciones restringidas. Para obtener más información, consulte Agregue una aplicación a la lista de aplicaciones restringidas.
	
	Lleve a cabo una de estas acciones:
	
	  • Para seleccionar aplicaciones mediante el nombre de la aplicación, haga clic en la opción Seleccionar aplicaciones de la lista de aplicaciones.
	  • Para seleccionar aplicaciones utilizando el ID de paquete de aplicación, haga clic en la opción Especifique el ID de paquete de aplicación. No debe utilizar el ID de paquete para agregar aplicaciones públicas. Agregue las aplicaciones públicas a la lista de aplicaciones restringidas y, a continuación, utilice la opción Seleccionar aplicaciones de la lista de aplicaciones para seleccionar las aplicaciones en su lugar.
	• Seleccione una aplicación integrada (solo dispositivos supervisados con iOS 9.3.2 y posteriores)
	
	Para eliminar una aplicación de la lista, haga clic en ✕.
	
	Cuando selecciona esta configuración y una aplicación restringida está instalada en un dispositivo iOS, se muestran un mensaje de advertencia y un enlace en la pestaña Dispositivos gestionados. Al hacer clic en el enlace, se muestra una lista de las aplicaciones que hacen que el dispositivo no cumpla los requisitos de conformidad.
	
	Para dispositivos supervisados con iOS 9.3.2 y posteriores, las acciones de cumplimiento para esta regla no son aplicables. Se impide automáticamente que los usuarios instalen aplicaciones restringidas.

Mostrar solo las aplicaciones permitidas en el dispositivo	Esta configuración crea una regla de conformidad que especifica una lista de aplicaciones que se pueden instalar en los dispositivos de los usuarios. El resto de aplicaciones no están permitidas. Para permitir aplicaciones específicas, realice una de las siguientes tareas: • Seleccione una aplicación de la lista de aplicaciones restringidas. Para obtener más información, consulte Agregue una aplicación a la lista de aplicaciones restringidas. • Seleccione una aplicación integrada (solo dispositivos supervisados con iOS 9.3.2 y posteriores) Algunas aplicaciones están incluidas en la lista de permitidos de manera predeterminada. Para eliminar una aplicación de la lista, haga clic en ✕. Esta configuración solo es válida para dispositivos supervisados con iOS 9.3.2 o posterior.

macOS: configuración del perfil de conformidad

Consulte Común: configuración del perfil de conformidad para obtener una explicación sobre las acciones posibles si se selecciona una regla de conformidad.

macOS: configuración del perfil de conformidad	Descripción
Versión de SO restringida instalada	Esta configuración crea una regla de conformidad para garantizar que los dispositivos no tienen una versión del SO restringida instalada según se especifica en esta configuración. Puede seleccionar las versiones del SO restringidas.
Modelo de dispositivo restringido detectado	Esta configuración crea una regla de conformidad para restringir modelos de dispositivo según se especifica en esta configuración. Valores posibles: • Permitir modelos de dispositivo seleccionados • No permitir modelos de dispositivo seleccionados Puede seleccionar los modelos de los dispositivos que están permitidos o restringidos.
Verificación de versiones de bibliotecas de BlackBerry Dynamics	Esta configuración crea una regla de conformidad que le permite seleccionar las versiones de bibliotecas de BlackBerry Dynamics que no se pueden activar. Puede seleccionar las versiones de bibliotecas bloqueadas.
Verificación de la conectividad de BlackBerry Dynamics	Esta configuración crea una regla de conformidad para garantizar que las aplicaciones de BlackBerry Dynamics no están fuera de contacto con BlackBerry UEM durante más de un periodo especificado. La acción de cumplimiento se aplica a las aplicaciones de BlackBerry Dynamics.
Basar intervalo de conectividad en las aplicaciones delegadas de la autenticación	Esta configuración especifica que la verificación de la conectividad se base en cuándo una aplicación delegada de autenticación se conecta a BlackBerry UEM. Esta configuración es válida únicamente si se ha seleccionado la opción "Verificación de la conectividad".

macOS: configuración del perfil de conformidad	Descripción
Última hora de contacto	Esta opción especifica el número de días para que el dispositivo deba conectarse a BlackBerry UEM. Valores posibles: • 8 horas • 16 horas • 1 día • 2 días • 3 días • 7 días • 14 días • 30 días • 60 días • 90 días • 180 días • 365 días El valor predeterminado es "2 días". Esta configuración es válida únicamente si se ha seleccionado la opción "Verificación de la conectividad".

Android: configuración del perfil de conformidad

Consulte Común: configuración del perfil de conformidad para obtener una explicación sobre las acciones posibles si se selecciona una regla de conformidad.

Android: configuración del perfil de conformidad	Descripción
SO con acceso a la raíz	Esta configuración crea una regla de conformidad para garantizar que los dispositivos no tienen acceso a la raíz. Un dispositivo tiene acceso a la raíz cuando un usuario o atacante obtiene acceso al nivel de raíz del Android OS.
La aplicación no asignada está instalada	Esta configuración crea una regla de conformidad para garantizar que los dispositivos no tienen aplicaciones instaladas que no se asignaron al usuario. Cuando selecciona esta configuración y una aplicación no asignada está instalada en un dispositivo con Android, se muestran un mensaje de advertencia y un enlace en la pestaña Dispositivos gestionados. Al hacer clic en el enlace, se muestra una lista de las aplicaciones que hacen que el dispositivo no cumpla los requisitos de conformidad. Para los dispositivos Android que tienen un perfil de trabajo y los dispositivos Samsung KNOX, los usuarios no pueden instalar aplicaciones no asignadas en el espacio de trabajo. Las acciones de cumplimiento no aplican. Esta configuración no es válida para dispositivos activados con Privacidad del usuario.

Android: configuración del perfil de conformidad	Descripción
La aplicación obligatoria no está instalada	Esta configuración crea una regla de conformidad para garantizar que los dispositivos tienen las aplicaciones necesarias instaladas. Cuando selecciona esta configuración y una aplicación obligatoria no está instalada en un dispositivo con Android, se muestran un mensaje de advertencia y un enlace en la pestaña Dispositivos gestionados. Al hacer clic en el enlace, se muestra una lista de las aplicaciones que hacen que el dispositivo no cumpla los requisitos de conformidad. Para los dispositivos Android que tienen un perfil de trabajo, no se aplican las acciones de cumplimiento. Para los dispositivos con Samsung KNOX, las aplicaciones internas requeridas se instalan automáticamente. Las acciones de cumplimiento solo se aplicarán a las aplicaciones públicas obligatorias.
Versión de SO restringida instalada	Esta configuración crea una regla de conformidad para garantizar que los dispositivos no tienen una versión del SO restringida instalada según se especifica en esta configuración. Puede seleccionar las versiones del SO restringidas.
Modelo de dispositivo restringido detectado	Esta configuración crea una regla de conformidad para restringir modelos de dispositivo según se especifica en esta configuración. Valores posibles: • Permitir modelos de dispositivo seleccionados • No permitir modelos de dispositivo seleccionados Puede seleccionar los modelos de los dispositivos que están permitidos o restringidos.
Dispositivo fuera de contacto	Esta configuración crea una regla de conformidad para garantizar que los dispositivos no están fuera de contacto con BlackBerry UEM durante más de un periodo especificado. El dispositivo verifica la conformidad con esta regla y puede eliminar datos de trabajo, eliminar todos los datos o desactivarse de BlackBerry UEM si no cumple los requisitos de conformidad.
Última hora de contacto	Esta configuración especifica el número de días que un dispositivo puede estar fuera de contacto con BlackBerry UEM. Esta configuración es válida únicamente si se ha seleccionado la opción "Dispositivo fuera de contacto".

Android: configuración del perfil de conformidad	Descripción
El nivel de revisión de seguridad requerido no está instalado.	Esta configuración crea una regla de conformidad para garantizar que los dispositivos tienen las revisiones de seguridad requeridas instaladas según se especifica en esta configuración. Puede especificar los modelos de dispositivos y las fechas de revisiones de seguridad. Los dispositivos que ejecutan una revisión de seguridad igual o posterior a las fechas de la revisión de seguridad especificada se consideran en cumplimiento. Esta configuración es válida únicamente para dispositivos con Android 6.0 y posterior, y dispositivos PRIV con Android 5.1.1 y posterior.
Verificación de versiones de bibliotecas de BlackBerry Dynamics	Esta configuración crea una regla de conformidad que le permite seleccionar las versiones de bibliotecas de BlackBerry Dynamics que no se pueden activar. Puede seleccionar las versiones de bibliotecas bloqueadas.
Verificación de la conectividad de BlackBerry Dynamics	Esta configuración crea una regla de conformidad para garantizar que las aplicaciones de BlackBerry Dynamics no están fuera de contacto con BlackBerry UEM durante más de un periodo especificado. La acción de cumplimiento se aplica a las aplicaciones de BlackBerry Dynamics.
Basar intervalo de conectividad en las aplicaciones delegadas de la autenticación	Esta configuración especifica que la verificación de la conectividad se base en cuándo una aplicación delegada de autenticación se conecta a BlackBerry UEM. Esta configuración es válida únicamente si se ha seleccionado la opción "Verificación de la conectividad".
Última hora de contacto	Esta opción especifica el número de días para que el dispositivo deba conectarse a BlackBerry UEM. Valores posibles: • 8 horas • 16 horas • 1 día • 2 días • 3 días • 7 días • 14 días • 30 días • 60 días • 90 días • 180 días • 365 días El valor predeterminado es "2 días".

Android: configuración del perfil de conformidad	Descripción
La aplicación restringida está instalada	Esta configuración crea una regla de conformidad para garantizar que los dispositivos no tienen las aplicaciones restringidas instaladas. Para restringir aplicaciones, consulte Agregue una aplicación a la lista de aplicaciones restringidas. Para los dispositivos Android que tienen un perfil de trabajo, los usuarios no pueden instalar aplicaciones restringidas en el espacio de trabajo. Las acciones de cumplimiento no se aplican. Para los dispositivos Samsung KNOX, las aplicaciones restringidas en el espacio de trabajo se desactivan automáticamente. Las acciones de cumplimiento no se aplican. Esta configuración no es válida para dispositivos activados con Privacidad del usuario. Cuando selecciona esta configuración y una aplicación restringida está instalada en un dispositivo con Android, se muestran un mensaje de advertencia y un enlace en la pestaña Dispositivos gestionados. Al hacer clic en el enlace, se muestra una lista de las aplicaciones que hacen que el dispositivo no cumpla los requisitos de conformidad.
La contraseña no cumple los requisitos de complejidad	Esta opción crea una regla de conformidad para asegurarse de que las contraseñas definidas por el usuario para el dispositivo o el espacio de trabajo cumplan los requisitos de conformidad definidos en la política de TI que tiene asignada.
Ejecutar acciones de cumplimiento en el espacio personal	Para los dispositivos Samsung KNOX, puede seleccionar este ajuste para evitar que los usuarios instalen una aplicación restringida en el espacio personal, así como en el espacio de trabajo.

Windows: configuración del perfil de conformidad

Consulte Común: configuración del perfil de conformidad para obtener una explicación sobre las acciones posibles si se selecciona una regla de conformidad.

Windows: configuración del perfil de conformidad	Descripción
La aplicación obligatoria no está instalada	Esta configuración crea una regla de conformidad para garantizar que los dispositivos tienen las aplicaciones necesarias instaladas. Las disposiciones de las aplicaciones internas solo se pueden controlar en dispositivos con Windows Phone 8.0. Cuando selecciona esta configuración y una aplicación obligatoria no está instalada en un dispositivo con Windows Phone, se muestran un mensaje de advertencia y un enlace en la pestaña Dispositivos gestionados. Al hacer clic en el enlace, se muestra una lista de las aplicaciones que hacen que el dispositivo no cumpla los requisitos de conformidad.

Windows: configuración del perfil de conformidad	Descripción
Versión de SO restringida instalada	Esta configuración crea una regla de conformidad para garantizar que los dispositivos no tienen una versión del SO restringida instalada según se especifica en esta configuración. Puede seleccionar las versiones del SO restringidas.
Modelo de dispositivo restringido detectado	Esta configuración crea una regla de conformidad para restringir modelos de dispositivo según se especifica en esta configuración. Valores posibles: • Permitir modelos de dispositivo seleccionados • No permitir modelos de dispositivo seleccionados Puede seleccionar los modelos de los dispositivos que están permitidos o restringidos.
Dispositivo fuera de contacto	Esta configuración crea una regla de conformidad para garantizar que los dispositivos no están fuera de contacto con BlackBerry UEM durante más de un periodo especificado.
Verificación de versiones de bibliotecas de BlackBerry Dynamics	Esta configuración crea una regla de conformidad que le permite seleccionar las versiones de bibliotecas de BlackBerry Dynamics que no se pueden activar. Puede seleccionar las versiones de bibliotecas bloqueadas.
Verificación de la conectividad de BlackBerry Dynamics	Esta configuración crea una regla de conformidad para garantizar que las aplicaciones de BlackBerry Dynamics no están fuera de contacto con BlackBerry UEM durante más de un periodo especificado. La acción de cumplimiento se aplica a las aplicaciones de BlackBerry Dynamics.
Firma de antivirus	Esta configuración crea una regla de conformidad para garantizar que los dispositivos tienen una firma de antivirus activada.
Estado del antivirus	Esta configuración crea una regla de conformidad para garantizar que los dispositivos tienen el software antivirus activado.
Estado del firewall	Esta configuración crea una regla de conformidad para garantizar que los dispositivos tienen un firewall activado.
Estado del cifrado	Esta configuración crea una regla de conformidad para garantizar que los dispositivos requieren cifrado.
Estado de actualización de Windows	Esta configuración crea una regla de conformidad para garantizar que los dispositivos permiten a BlackBerry UEM instalar actualizaciones del sistema operativo Windows o notificar a los usuarios las actualizaciones necesarias.

Windows: configuración del perfil de conformidad	Descripción
La aplicación restringida está instalada	Esta configuración crea una regla de conformidad para garantizar que los dispositivos no tienen las aplicaciones restringidas instaladas. Para restringir aplicaciones, consulte Agregue una aplicación a la lista de aplicaciones restringidas. Esta configuración es válida para dispositivos con Windows Phone 8.1 y posterior.
Periodo de gracia caducado	Esta configuración crea una regla de conformidad que le permite especificar las acciones que se llevan a cabo si se agota el periodo de gracia de la atestación.
Clave de identidad de la atestación no existente	Esta configuración crea una regla de conformidad que le permite especificar las acciones que se llevan a cabo si no hay una AIK presente en el dispositivo.
La política Prevención de ejecución de datos está desactivada	Esta configuración crea una regla de conformidad que le permite especificar las acciones que se llevan a cabo si la política DEP está desactivada en el dispositivo.
BitLocker está desactivado	Esta configuración crea una regla de conformidad que le permite especificar las acciones que se llevan a cabo si BitLocker está desactivado en el dispositivo.
El arranque seguro está desactivado	Esta configuración crea una regla de conformidad que le permite especificar las acciones que se llevan a cabo si el arranque seguro está desactivado en el dispositivo.
La integridad del código está desactivada	Esta configuración crea una regla de conformidad que le permite especificar las acciones que se llevan a cabo si la función de integridad del código está desactivada en el dispositivo.
El dispositivo está en modo seguro	Esta configuración crea una regla de conformidad que le permite especificar las acciones que se llevan a cabo si el dispositivo está en modo seguro.
El dispositivo está en el entorno de preinstalación de Windows	Esta configuración crea una regla de conformidad que le permite especificar las acciones que se llevan a cabo si el dispositivo está en el entorno de preinstalación de Windows.
El controlador antimalware de inicio temprano no está cargado	Esta configuración crea una regla de conformidad que le permite especificar las acciones que se llevan a cabo si el controlador antimalware de inicio temprano no está cargado.
El modo seguro virtual está desactivado	Esta configuración crea una regla de conformidad que le permite especificar las acciones que se llevan a cabo si el modo seguro virtual está desactivado.
La depuración de arranque está activada	Esta configuración crea una regla de conformidad que le permite especificar las acciones que se llevan a cabo si la depuración de arranque está activada.
La depuración del kernel del SO está activada	Esta configuración crea una regla de conformidad que le permite especificar las acciones que se llevan a cabo si el kernel del SO está activado.

Windows: configuración del perfil de conformidad	Descripción
La firma de pruebas está activada	Esta configuración crea una regla de conformidad que le permite especificar las acciones que se llevan a cabo si la firma de pruebas está activada.
La lista de revisiones del administrador de arranque no tiene la versión esperada	Esta configuración crea una regla de conformidad que le permite especificar las acciones que se llevan a cabo si la lista de revisiones del administrador de arranque no tiene la versión esperada.
La lista de revisiones de la integridad de código no tiene la versión esperada	Esta configuración crea una regla de conformidad que le permite especificar las acciones que se llevan a cabo si la lista de revisiones de la integridad de código no tiene la versión esperada.
El hash de la política Integridad de código está presente y no tiene un valor permitido	Esta configuración crea una regla de conformidad que le permite especificar las acciones que se llevan a cabo si el hash de la política Integridad de código no está presente y no tiene un valor permitido.
El hash de la política de configuración de arranque seguro personalizado está presente y no tiene un valor permitido	Esta configuración crea una regla de conformidad que le permite especificar las acciones que se llevan a cabo si el hash de la política de configuración de arranque seguro personalizado no está presente y no tiene un valor permitido.
El valor de PCR no es un valor permitido	Esta configuración crea una regla de conformidad que le permite especificar las acciones que se llevan a cabo si el valor de PCR no es un valor permitido.

Ajustes del perfil de BlackBerry Dynamics

Los perfiles de BlackBerry Dynamics son compatibles con los siguientes tipos de dispositivos:

- iOS
- Android
- macOS
- Windows

Configuración de perfil de BlackBerry Dynamics	Descripción
Configuración	
Requerir la gestión de dispositivos para usar aplicaciones de BlackBerry Dynamics	Esta configuración especifica si un dispositivo debe activarse con MDM para utilizar las aplicaciones de BlackBerry Dynamics.

Configuración de perfil de BlackBerry Dynamics	Descripción
Activar UEM Client para que pueda inscribirse en BlackBerry Dynamics	Si un dispositivo está utilizando BlackBerry UEM Client, esta configuración especifica si BlackBerry Dynamics gestiona la activación de las aplicaciones de BlackBerry Dynamics y si las aplicaciones de BlackBerry Dynamics se pueden utilizar en el dispositivo. Si no se selecciona esta opción, las aplicaciones de BlackBerry Dynamics se pueden eliminar del dispositivo porque este no estará activado para BlackBerry Dynamics. Si no planea usar BlackBerry Dynamics en su entorno, no seleccione esta opción.
Contraseña	
Caducidad de la contraseña	Esta configuración especifica si la contraseña de una aplicación de BlackBerry Dynamics caduca y el número de días que una contraseña sigue siendo válida antes de que caduque.
No permitir contraseñas anteriores	Esta configuración especifica si se pueden utilizar las contraseñas anteriores y el número máximo de contraseñas anteriores que no pueden utilizarse para una aplicación de BlackBerry Dynamics.
Longitud mínima de la contraseña:	Esta configuración especifica la longitud mínima de la contraseña para una aplicación de BlackBerry Dynamics.
Repeticiones permitidas de un carácter	Esta configuración especifica el número de veces que un carácter puede aparecer en una contraseña para una aplicación de BlackBerry Dynamics.
Requerir letras y números	Esta configuración especifica si la contraseña debe contener letras y números para una aplicación de BlackBerry Dynamics.
Requerir mayúsculas y minúsculas	Esta configuración especifica si la contraseña debe contener letras mayúsculas y minúsculas para una aplicación de BlackBerry Dynamics.
Requerir al menos un carácter especial	Esta configuración especifica si la contraseña debe contener al menos un carácter especial para una aplicación de BlackBerry Dynamics.
No permitir secuencias de más de dos números	Esta configuración especifica si la contraseña puede contener más de dos números secuenciales (como 1, 2, 3) para una aplicación de BlackBerry Dynamics.
No permitir más de un cambio de contraseña al día	Esta configuración especifica si la contraseña se puede cambiar más de una vez cada 24 horas para una aplicación de BlackBerry Dynamics.
No permitir información personal	Esta configuración especifica si la siguiente información personal se puede utilizar en una contraseña para una aplicación de BlackBerry Dynamics: • Los apellidos y nombre del usuario (excluidas las iniciales) como se registraron en Active Directory. • La parte de una dirección de correo electrónico antes del signo @.

Configuración de perfil de BlackBerry Dynamics	Descripción
Permitir Biometría	Esta configuración especifica si las aplicaciones de BlackBerry Dynamics pueden desbloquearse mediante datos biométricos cuando ya están abiertas en el conmutador de aplicaciones en los dispositivos iOS. Puede permitir las siguientes opciones: • Ninguno • Permitir Touch ID • Permitir Face ID • Permitir Touch ID y Face ID
Activar Touch ID y Face ID con arranque en frío	Esta configuración especifica si las aplicaciones de BlackBerry Dynamics pueden desbloquearse mediante los métodos de datos biométricos seleccionados la primera vez que se abren después de reiniciar el dispositivo.
Requerir que la contraseña vuelva a introducirse y desactivar Touch ID y Face ID	Esta configuración especifica un periodo de tiempo tras el cual los usuarios deben introducir una contraseña para desbloquear una aplicación de BlackBerry Dynamics y volver a activar Touch ID, Face ID o ambos.
Permitir la autenticación mediante huella digital de Android	Esta configuración especifica si las aplicaciones de BlackBerry Dynamics pueden desbloquearse utilizando la autenticación mediante huella digital de Android.
No requiere contraseña	Esta configuración especifica si un usuario puede acceder a una aplicación de BlackBerry Dynamics sin introducir una contraseña. Las opciones son las siguientes: • iOS • macOS • Android • Windows
Lista de contraseñas bloqueadas	
Archivo de contraseñas bloqueadas (.txt)	Esta configuración especifica una lista de contraseñas prohibidas. Puede descargar la lista de contraseñas prohibidas cargadas anteriormente. Las contraseñas de la lista deben cumplir los requisitos siguientes: cada contraseña debe estar separada por un retorno de carro, solo se admiten caracteres UTF-8 y las contraseñas deben tener 14 caracteres o menos.
Pantalla de bloqueo	
Requerir contraseña al iniciar aplicaciones de BlackBerry Dynamics	Esta configuración especifica si se requiere una contraseña cada vez que se inicia una aplicación de BlackBerry Dynamics. **Nota:** Si está utilizando la delegación de autenticación, no seleccione esta opción.
Requerir contraseña tras periodo de inactividad	Esta configuración especifica el periodo de inactividad que debe transcurrir para que se requiera la contraseña.

Configuración de perfil de BlackBerry Dynamics	Descripción
Realizar acción tras intentos de contraseña no válidos	Esta configuración especifica si existe un límite del número de veces que un usuario puede introducir una contraseña incorrecta. Si selecciona esta regla, especifique el número de veces que un usuario puede introducir una contraseña incorrecta y lo que ocurre después de haber alcanzado el límite. Elija una de las siguientes acciones: • Bloquear usuario • Borrar datos
Accesorios	
Permitir accesorios	Esta configuración especifica si las aplicaciones de BlackBerry Dynamics se pueden utilizar en un dispositivo portátil. Si selecciona esta regla, especifique cuánto tiempo debe transcurrir para que el dispositivo portátil se desconecte y si se puede volver a conectar automáticamente.
Delegación de autenticación de aplicaciones	

Configuración de perfil de BlackBerry Dynamics	Descripción
	Puede designar una aplicación de BlackBerry Dynamics para que actúe como delegado de la autenticación en nombre de otras aplicaciones de BlackBerry Dynamics, de modo que los usuarios no tengan que crear una contraseña para cada aplicación de BlackBerry Dynamics que instalan. Una vez que la delegación de la autenticación se haya configurado, cada vez que un usuario abra una aplicación de BlackBerry Dynamics, el dispositivo mostrará la pantalla de la contraseña de la delegada de la autenticación en lugar de la aplicación que intenta abrir. Después de que el usuario introduzca la contraseña para la delegada de la autenticación, podrá abrir la aplicación de BlackBerry Dynamics. Puede elegir cualquier aplicación para que actúe como delegada de la autenticación para otras aplicaciones, pero se recomienda que elija la aplicación utilizada con más frecuencia para que actúe como la delegada de la autenticación principal a fin de ofrecer la experiencia más sencilla para el usuario. Como práctica recomendada, se recomienda establecer un solo delegado de autenticación. Esto evita cambios innecesarios de delegado de autenticación, complejos y no deseados, y simplifica la gestión administrativa. Si un usuario elimina accidentalmente el delegado de autenticación, debe volver a instalarlo. Si se requiere más de un delegado de autenticación, por ejemplo, el delegado de autenticación principal no existe para una plataforma determinada y se configurar un delegado alternativo, consulte las recomendaciones siguientes para asegurarse de que las aplicaciones de BlackBerry Dynamics se instalan y activan correctamente: • Los usuarios deben instalar siempre el delegado de autenticación principal en primer lugar y no deben activarlo utilizando una aplicación delegada de autenticación alternativa ya instalada. • Si el usuario ya tiene un delegado de autenticación alternativo instalado y en uso, y posteriormente instala el delegado de autenticación principal, deberá asegurarse de que el delegado de autenticación instalado existente está desbloqueado para completar correctamente la autenticación. Si se ha forzado el cierre del delegado de autenticación alternativo, el usuario encontrará varios errores y puede que se bloquee. • Los usuarios no deben eliminar el delegado de autenticación ya instalado después de instalar el delegado de autenticación principal. Las aplicaciones que utilizan actualmente el delegado de autenticación deberán cambiar automáticamente al nuevo delegado de autenticación cuando la aplicación se inicie la próxima vez en modo en línea. • Si se elimina el delegado de autenticación principal, los usuarios deben volver a activar el delegado de autenticación utilizando una clave de acceso. Si intentan activar el delegado de autenticación con otra aplicación, pueden aparecer varios errores. • Incluso si se selecciona la opción para "permitir la autoautenticación" o si se instala una aplicación designada como delegado de autenticación secundario o terciario, no existe un mecanismo de reconexión para permitir que las aplicaciones cambien el delegado de autenticación sin instalar y desbloquear el delegado de autenticación original.

Configuración de perfil de BlackBerry Dynamics	Descripción
Prevención de fugas de datos	
No permitir la copia de datos de aplicaciones que no sean de BlackBerry Dynamics en aplicaciones de BlackBerry Dynamics	Esta configuración especifica si los usuarios pueden copiar datos de aplicaciones que no sean de BlackBerry Dynamics a aplicaciones de BlackBerry Dynamics. **Nota:** Si utiliza una solución PKI basada en aplicación, como Purebred, no seleccione esta opción.
No permitir dictado de Android	Esta configuración especifica si los usuarios de dispositivos Android pueden utilizar dictado por voz con las aplicaciones de BlackBerry Dynamics.
No permitir capturas de pantalla en dispositivos Android	Esta configuración especifica si los usuarios de dispositivos Android pueden realizar capturas de pantalla en aplicaciones de BlackBerry Dynamics.
No permitir grabar y compartir pantalla en dispositivos iOS	Esta configuración especifica si los usuarios de dispositivos iOS pueden compartir y grabar pantallas en aplicaciones de BlackBerry Dynamics. Esta configuración se aplica a los dispositivos con iOS 11 y posteriores.
No permitir dictado de iOS	Esta configuración especifica si los usuarios de dispositivos iOS pueden utilizar dictado por voz con las aplicaciones de BlackBerry Dynamics.
No permitir teclados personalizados en dispositivos iOS	Esta configuración especifica si los usuarios de dispositivos iOS pueden utilizar teclados personalizados con aplicaciones de BlackBerry Dynamics.
Activar FIPS	Esta configuración especifica si se aplica la conformidad con el estándar federal estadounidense de procesamiento de la información 140-2.
Certificados	
Activar almacén de certificados de dispositivo	Esta configuración especifica si las aplicaciones de BlackBerry Dynamics pueden obtener certificados del almacén de certificados de dispositivos.
Registro detallado	
Activar el registro detallado para las aplicaciones de BlackBerry Dynamics	En la configuración se especifica si los archivos de registro se pueden generar y cargar desde aplicaciones de BlackBerry Dynamics.
Evitar que los usuarios activen el registro detallado en las aplicaciones de BlackBerry Dynamics	En la configuración se especifica si los usuarios pueden activar la capacidad para generar y compartir archivos de registro detallados de aplicaciones de BlackBerry Dynamics.

Configuración de perfil de BlackBerry Dynamics	Descripción
Contrato	
Activar un mensaje de contrato para aplicaciones de BlackBerry Dynamics	Esta configuración específica si se debe mostrar un mensaje en las aplicaciones de BlackBerry Dynamics que el usuario debe confirmar. Si la delegación de la autenticación está activada, el mensaje solo aparece en la aplicación del autenticador. Si selecciona esta regla, realice las siguientes acciones: • Especifique si se muestra el mensaje cada vez que la aplicación se desbloquee; de lo contrario, el mensaje solo aparece la primera vez que el usuario abre la aplicación. • En el campo **Mensaje**, cree el mensaje que desea visualizar. **Nota:** En los dispositivos Android, solo se muestran los primeros 4000 caracteres.

Configuración del perfil de conectividad de BlackBerry Dynamics

Los perfiles de conectividad de BlackBerry Dynamics son compatibles con los siguientes tipos de dispositivos:

- iOS
- Android
- macOS
- Windows

Configuración del perfil de conectividad de BlackBerry Dynamics	Descripción
Importación del perfil de conectividad de BlackBerry Dynamics	Haga clic en el icono para importar la configuración de conectividad desde un archivo .csv. Cuando importa un archivo .csv, este sustituye los contenidos del perfil de conectividad. Esto facilita la edición manual de los valores o si es necesario modificar varias URL o varios servidores.
Exportación del perfil de conectividad de BlackBerry Dynamics	Haga clic en para exportar la configuración de conectividad a un archivo .csv.
Infraestructura	
Distribuir todo el tráfico	Especifique si todos los datos de las aplicaciones de BlackBerry Dynamics se enrutan a través de BlackBerry Proxy. Para obtener más información, consulte Enrutamiento de todos los datos de aplicaciones de BlackBerry Dynamics a través de BlackBerry Proxy.

Configuración del perfil de conectividad de BlackBerry Dynamics	Descripción
Dominio	Especifique los dominios de Internet a los que desea permitir el acceso. Por ejemplo, `blackberry.com` permite acceder a cualquier servidor en el dominio blackberry.com. BlackBerry Dynamics Las aplicaciones de <1/> pueden conectarse a través del firewall de su empresa a cualquier servidor en los dominios indicados y en sus subdominios.
Clústeres primarios y secundarios de BlackBerry Proxy	Especifique el nombre de dominio completo, el puerto y la prioridad de los clústeres de BlackBerry Proxy que deben utilizarse para acceder al dominio.
Dominios predeterminados	
Dominio	Especifique el valor de dominios permitidos predeterminado (por ejemplo, qa.blackberry.com). Es posible que las aplicaciones de BlackBerry Dynamics intenten conectarse a un nombre de host incompleto como "portal" en lugar de usar el nombre completo como "portal.sales.xyzcorp.com". Los dominios de esta lista se anexan a los nombres de host incompletos para formar nombres completos.
Servidores adicionales	
Servidor	Especifique el nombre de dominio completo de los servidores adicionales a los que las aplicaciones de BlackBerry Dynamics pueden conectarse. Agregue servidores a esta lista en lugar de usar la lista "Dominios permitidos" si desea que las aplicaciones de BlackBerry Dynamics se conecten únicamente a determinados servidores y no a todos los servidores de un dominio.
Intervalos de direcciones IP	
Intervalo	Especifique un rango de direcciones IP a las que las aplicaciones de BlackBerry Dynamics pueden acceder. Los rangos de direcciones se deben introducir con la dirección inferior y superior (por ejemplo, 192.168.2.0-192.168.2.255) o en notación IPv4 CIDR (por ejemplo, 192.168.2.0/24). Por ejemplo: • Direcciones separadas: Ejemplo: 192.168.2.0-192.168.2.255 • Toda una subred: Ejemplo: 192.168.2.0/24
Servidores de aplicaciones	Si tiene una aplicación de BlackBerry Dynamics proporcionada desde un servidor de aplicaciones o un servidor web, puede especificar el nombre de dicho servidor y la prioridad de los clústeres de BlackBerry Proxy utilizados para la comunicación. Para obtener más información, consulte Adición de un servidor de aplicaciones a un perfil de conectividad de BlackBerry Dynamics.

Configuración del perfil de conectividad de empresa

Los perfiles de conectividad de empresa son compatibles con los siguientes tipos de dispositivos:

- BlackBerry 10
- iOS
- Android

Común: configuración del perfil de conectividad de empresa

Común: configuración del perfil de conformidad	Descripción
Grupo de servidores de BlackBerry Secure Connect Plus	Esta configuración especifica el grupo de servidores que utiliza BlackBerry Secure Connect Plus para dirigir el tráfico a una ruta regional específica. Esta configuración es válida únicamente si ha instalado una o más instancias de BlackBerry Connectivity Node y configurado los grupos de servidores.

BlackBerry 10: configuración del perfil de conectividad de empresa

Configuración	Descripción
Conectividad de la empresa	La conectividad de la empresa siempre está activada para los dispositivos con BlackBerry 10. No puede cambiar esta configuración.
Perfil de proxy	Esta configuración especifica el perfil de proxy asociado si desea enrutar el tráfico de túnel seguro de los dispositivos a la red del trabajo a través de un servidor proxy.
Activar BlackBerry Secure Connect Plus	Esta configuración especifica si las aplicaciones de trabajo utilizan BlackBerry Secure Connect Plus para enviar los datos de trabajo entre los dispositivos y la red.

iOS: configuración del perfil de conectividad de empresa

Configuración	Descripción
Activar BlackBerry Secure Connect Plus	Esta configuración especifica si las aplicaciones de trabajo utilizan BlackBerry Secure Connect Plus para enviar los datos de trabajo entre los dispositivos y la red.
Activar VPN a petición	Esta configuración especifica si una aplicación de trabajo puede iniciar una conexión VPN utilizando BlackBerry Secure Connect Plus cuando accede a los recursos de trabajo. Seleccione esta configuración para especificar reglas para las conexiones de BlackBerry Secure Connect Plus.

Configuración	Descripción
Reglas de VPN a petición para iOS 9 y posteriores	Esta configuración especifica los requisitos de conexión para VPN a petición utilizando BlackBerry Secure Connect Plus. Debe utilizar una o más claves del ejemplo de formato de carga. Esta configuración es válida únicamente si se ha seleccionado la opción "Activar VPN a petición".
Activar VPN por aplicación	Seleccione esta comunicación para permitir que solo aplicaciones específicas utilicen BlackBerry Secure Connect Plus. **Nota:** Si selecciona esta opción, los usuarios deben activar manualmente la conexión VPN en su dispositivo para utilizar BlackBerry Secure Connect Plus. Mientras la conexión VPN está activada, el dispositivo utiliza BlackBerry Secure Connect Plus para conectarse a la red del trabajo. El usuario debe activar la conexión VPN para utilizar otra conexión, como la red Wi-Fi del trabajo. Indique a los usuarios cuándo es el momento adecuado para activar y desactivar la conexión VPN (por ejemplo, puede indicarles que activen la conexión VPN cuando no están dentro del alcance de la red Wi-Fi del trabajo).
Dominios de Safari	Haga clic en + para especificar los dominios que tienen permitido iniciar una conexión VPN en Safari.
Permitir la conexión automática de aplicaciones	Especifique si las aplicaciones pueden iniciar automáticamente la conexión VPN.
Perfil de proxy	Esta configuración especifica el perfil de proxy asociado si desea enrutar el tráfico de túnel seguro de los dispositivos a la red del trabajo a través de un servidor proxy. El perfil de proxy debe utilizar una configuración manual con una dirección IP. No se admite la configuración de PAC. Para obtener más información, consulte Configuración de los perfiles de proxy para dispositivos.

Android: configuración del perfil de conectividad de empresa

Configuración	Descripción
Activar BlackBerry Secure Connect Plus	Esta configuración especifica si las aplicaciones de trabajo utilizan BlackBerry Secure Connect Plus para enviar los datos de trabajo entre los dispositivos y la red.
Conectividad de la empresa para dispositivos Android con un espacio de trabajo	Esta configuración especifica si el perfil de trabajo de Android y los dispositivos Samsung KNOX Workspace utilizan BlackBerry Secure Connect Plus para todas las aplicaciones del espacio de trabajo o solo para las aplicaciones especificadas. • "VPN de todo el contenedor" utiliza una conexión VPN para todas las aplicaciones del espacio de trabajo en el dispositivo. • "VPN por aplicación" utiliza una conexión VPN solo para aplicaciones específicas.

Configuración	Descripción
Aplicaciones con uso restringido de BlackBerry Secure Connect Plus	Esta configuración especifica las aplicaciones del espacio de trabajo en dispositivos de perfil de trabajo Android que no pueden utilizar BlackBerry Secure Connect Plus. Haga clic en + y escriba el ID de paquete de aplicación. Repita según sea necesario para restringir aplicaciones adicionales. De forma predeterminada, Google Play y los servicios subyacentes (com.android.providers.media, com.android.vending, com.google.android.gms y com.google.android.apps.gcs) están restringidos porque Google Play no cuenta con soporte de proxy. Se recomienda mantener estas restricciones. Si elimina cualquiera de estas restricciones, debe ponerse en contacto con el soporte de Google Play para conocer la configuración de cortafuegos necesaria para permitir las conexiones a Google Play mediante BlackBerry Secure Connect Plus. Si se aplica la política de TI "Forzar que las aplicaciones de trabajo solo utilicen VPN" al dispositivo, esta configuración se ignora y no se impide que las aplicaciones de trabajo, incluidas las aplicaciones BlackBerry UEM Client y Google Play utilicen BlackBerry Secure Connect Plus. En ese caso, deberá abrir los puertos del firewall para permitir que BlackBerry UEM Client se comunique con BlackBerry Infrastructure a través de BlackBerry UEM. Para obtener más información acerca de cómo abrir los puertos del firewall cuando se utilizan aplicaciones de trabajo BlackBerry Secure Connect Plus, visite http://support.blackberry.com/kb para leer el artículo KB48330. Si su empresa utiliza aplicaciones de BlackBerry Dynamics, se recomienda que restrinja que las aplicaciones usen BlackBerry Secure Connect Plus. De lo contrario, debe abrir puertos adicionales en el firewall de su empresa para permitir que las aplicaciones envíen datos a BlackBerry Dynamics NOC, y la actividad de red de las aplicaciones puede retrasarse debido a que los datos se enrutan a BlackBerry Infrastructure y BlackBerry Dynamics NOC. Esta configuración es válida únicamente si la configuración "Conectividad de la empresa para dispositivos Android con un espacio de trabajo" se establece en "VPN de todo el contenedor".
Aplicaciones con permiso para usar Enterprise Connectivity	Esta configuración especifica las aplicaciones del espacio de trabajo en el perfil de trabajo de Android y los dispositivos Samsung KNOX Workspace que pueden utilizar BlackBerry Secure Connect Plus. Puede seleccionar aplicaciones en una lista de aplicaciones disponibles o especificar el ID de paquete de aplicación. Esta configuración es válida únicamente si la configuración "Conectividad de la empresa para dispositivos Android con un espacio de trabajo" se establece en "VPN por aplicación".
Perfil de proxy	Si desea enrutar el tráfico de túnel seguro de los dispositivos con Samsung KNOX Workspace 2.5 o posteriores a la red del trabajo a través de un servidor proxy, seleccione el perfil de proxy adecuado. Esta configuración no se aplica a los dispositivos Android que utilizan un perfil de trabajo ni a los dispositivos con Samsung KNOX Workspace versión 2.4 y anteriores.

Ajustes del perfil de Enterprise Management Agent

Los perfiles de Enterprise Management Agent son compatibles con los siguientes tipos de dispositivos:

- BlackBerry 10
- iOS
- Android
- Windows

BlackBerry 10: ajustes del perfil de Enterprise Management Agent

Configuración	Descripción
Intervalo de sondeo de Enterprise Management Web Service	Especifique con qué frecuencia, en segundos, desea que Enterprise Management Web Service en el dispositivo busque actualizaciones de configuración. Valores posibles: • De 3600 a 86400 El valor predeterminado es 3600.
Intervalo de sondeo rápido	Especifique con qué frecuencia, en segundos, desea que el dispositivo busque actualizaciones cuando la notificación de inserción no esté disponible para el sondeo rápido (BPDS no está registrado). • Mínimo: 900 El valor predeterminado es 900.
Intervalo de sondeo lento	Especifique con qué frecuencia, en segundos, desea que el dispositivo busque actualizaciones cuando la notificación de inserción esté disponible para el sondeo lento (BPDS está registrado). • Mínimo: 900 El valor predeterminado es 900.
Permitir colecciones de aplicaciones personales	Esta opción especifica si desea que BlackBerry UEM reciba una lista de las aplicaciones personales que están instaladas en los dispositivos de los usuarios. Esta opción no es compatible con los dispositivos con activaciones corporativas de trabajo y personales.

Configuración	Descripción
Archivo de configuración (*.json)	Esta configuración le permite especificar un archivo de configuración para restringir los paquetes de cifrado de la biblioteca SSL compatibles con el dispositivo. Especifique un archivo de configuración solo si desea eliminar la compatibilidad con un paquete de cifrado que tenga una vulnerabilidad de seguridad y los recursos de su empresa no requieren ese paquete de cifrado para la comunicación. La especificación de un archivo de configuración no afecta a la comunicación del dispositivo con BlackBerry UEM, pero podría afectar a la comunicación con otros servidores de la empresa, en función de los requisitos de dichos servidores. El archivo de configuración debe tener formato .json. **Ejemplo:** `{"tls": {"tls_protocols": ["TLSv1"], "tls_ciphersuites": [49200, 49196, 49192, 49188, 49172, 49162, 163, 159, 107, 106, 57, 56, 136, 135, 49202, 49198, 49194, 49190, 49167, 49157, 157, 61, 53, 132, 141, 49199, 49195, 49191, 49187, 49171, 49161, 162, 158, 103, 64, 51, 50, 154, 153, 69, 68, 49201, 49197, 49193, 49189, 49166, 49156, 156, 60, 47, 150, 65, 140, 49169, 49159, 49164, 49154, 5, 4, 138, 49170, 49160, 22, 19, 49165, 49155, 10, 139, 21, 18, 9, 20, 17, 8, 6, 3], "tls_curves": ["secp256r1", "secp521r1", "brainpoolP512r1", "brainpoolP384r1", "secp384r1", "brainpoolP256r1", "secp256k1", "sect571r1", "sect571k1", "sect409k1", "sect409r1", "sect283k1", "sect283r1", "secp224k1", "secp224r1", "secp192k1", "secp192r1", "secp160k1", "secp160r1", "secp160r2", "sect239k1", "sect233k1", "sect233r1", "sect193r1", "sect193r2", "sect163k1", "sect163r1", "sect163r2"], "tls_sigalgs": ["ECDSA+SHA512", "DSA+SHA512", "RSA+SHA512", "ECDSA +SHA384", "DSA+SHA384", "RSA+SHA384", "ECDSA+SHA256", "DSA +SHA256", "RSA+SHA256", "ECDSA+SHA224", "DSA+SHA224", "RSA+SHA224", "ECDSA+SHA1", "DSA+SHA1", "RSA+SHA1"], "tls_dh_min_key_bits":768, "tls_suiteb_mode": "SUITEB_OFF"}, "vpn": {"vpn_encr": ["aes128", "aes256", "aes128_icv16_gcm", "aes256_icv16_gcm", "3des", "aes192"], "vpn_dh": ["dh2", "dh5", "dh7", "dh8", "dh9", "dh10", "dh11", "dh12", "dh13", "dh14", "dh15", "dh16", "dh17", "dh18", "dh19", "dh20", "dh21", "dh22", "dh23", "dh24", "dh25", "dh26"], "vpn_integ": ["sha1", "sha384", "sha512", "aes", "sha256"], "vpn_prf": ["sha1", "sha384", "sha512", "aes", "hmac", "sha256"]}}`

iOS: ajustes del perfil de Enterprise Management Agent

Configuración	Descripción
Frecuencia de sondeo de Enterprise Management Agent	Especifique con qué frecuencia, en segundos, desea que el dispositivo busque comandos de servidor de Enterprise Management Agent. Valores posibles: • De 900 a 86400 El valor predeterminado es 3600.
Permitir colecciones de aplicaciones personales	Esta opción especifica si desea que BlackBerry UEM reciba una lista de las aplicaciones personales que están instaladas en los dispositivos de los usuarios. Esta opción no es compatible con los dispositivos con activaciones de privacidad del usuario.

Android: ajustes del perfil de Enterprise Management Agent

Configuración	Descripción
Cambios de la aplicación	Especifique con qué frecuencia, en segundos, desea que el dispositivo busque los cambios de las aplicaciones instaladas. Valores posibles: • De 3600 a 86400 segundos El valor predeterminado es 3600.
Umbral del nivel de batería	Especifique el cambio en el porcentaje de nivel de batería (de 5 a 100) obligatorio antes de que el dispositivo envíe la información de nuevo a BlackBerry UEM. Valores posibles: • Del 5 al 100 por ciento El valor predeterminado es 20.
Umbral de espacio libre de RAM	Especifique el cambio requerido en la cantidad de memoria libre en megabytes antes de que el dispositivo envíe la información de nuevo a BlackBerry UEM. De manera predeterminada, el dispositivo no envía esta información de nuevo a BlackBerry UEM.
Umbral del almacenamiento interno	Especifique el cambio requerido en la cantidad de espacio de almacenamiento interno libre en megabytes antes de que el dispositivo envíe la información de nuevo a BlackBerry UEM. El valor predeterminado es 250.
Umbral de la tarjeta de memoria	Especifique el cambio requerido en la cantidad de espacio externo libre (en megabytes) antes de que el dispositivo envíe la información de nuevo a BlackBerry UEM . El valor predeterminado es 500.

Configuración	Descripción
Frecuencia de sondeo de Enterprise Management Agent	Especifique con qué frecuencia, en segundos, desea que el dispositivo busque comandos de servidor de Enterprise Management Agent. Valores posibles: • Mínimo: 900 El valor predeterminado es 900.
Permitir colecciones de aplicaciones personales	Esta opción especifica si desea que BlackBerry UEM reciba una lista de las aplicaciones personales que están instaladas en los dispositivos de los usuarios. Esta opción no es compatible con los dispositivos con activaciones de privacidad del usuario.

Windows: ajustes del perfil de Enterprise Management Agent

Configuración	Descripción
Intervalo de sondeo para las actualizaciones de configuración de los dispositivos	Especifique en minutos con qué frecuencia desea que el dispositivo busque actualizaciones cuando la notificación de inserción no esté disponible.
Intervalo de sondeo para el primer conjunto de reintentos	Especifique el tiempo en minutos que debe esperarse entre intentos para el primer conjunto de reintentos si falla la búsqueda de actualizaciones para la configuración del dispositivo.
Número de primeros reintentos	Especifique el número de intentos del primer conjunto de reintentos.
Intervalo de sondeo para el segundo conjunto de reintentos	Especifique el tiempo en minutos que debe esperarse entre intentos para el segundo conjunto de reintentos si falla la búsqueda de actualizaciones para la configuración del dispositivo.
Número de segundos reintentos	Especifique el número de intentos del segundo conjunto de reintentos.
Intervalo de sondeo de los reintentos programados restantes	Especifique el tiempo en minutos que debe esperarse entre los intentos sucesivos después del segundo conjunto de reintentos si falla la búsqueda de actualizaciones para la configuración del dispositivo.
Número de reintentos programados restantes	Especifique el número de intentos sucesivos después del segundo conjunto de reintentos si falla la búsqueda de actualizaciones para la configuración del dispositivo. Si se ajusta a "0", el dispositivo continuará realizando sondeos hasta que se establezca una conexión correctamente o hasta que se desactive el dispositivo.
Sondeo en inicio de sesión de usuario	Especifique si el dispositivo debe iniciar una sesión de administración siempre que un usuario inicie sesión.

Configuración	Descripción
Sondeo de todos los usuarios en el primer inicio de sesión	Especifique si el dispositivo debe iniciar una sesión de administración la primera vez que inicien sesión todos los usuarios.
Permitir colecciones de aplicaciones personales	Esta opción especifica si desea que BlackBerry UEM reciba una lista de las aplicaciones personales que están instaladas en los dispositivos de los usuarios.

Configuración del perfil de Windows Information Protection

Los perfiles de Windows Information Protection son compatibles con los siguientes tipos de dispositivos:

- Windows 10

Windows 10: configuración de perfil de Windows Information Protection

Windows 10: configuración de perfil de Windows Information Protection	Descripción
Configuración de Windows Information Protection	Esta configuración especifica si se ha activado Windows Information Protection y el nivel de aplicación. Cuando esta configuración está definida en "Desactivado", no se cifran los datos y se desactiva el registro de auditoría. Cuando esta configuración se establece en "Silencio", los datos se cifran y se registra cualquier intento de compartir datos protegidos. Cuando esta configuración se establece en "Anulación", los datos se cifran, se avisa al usuario cuando intenta compartir datos protegidos y se registra cualquier intento de compartir datos protegidos. Cuando esta configuración se establece en "Bloqueo", los datos se cifran, los usuarios no pueden compartir datos protegidos y se registra cualquier intento de compartir datos protegidos. Valores posibles: • Desactivado • Silencio • Anulación • Bloqueo El valor predeterminado es "Desactivado".
Nombres de dominio protegidos de la empresa	Esta configuración especifica los nombres de dominio de la red de trabajo que utiliza su empresa para las identidades de usuario. Puede separar varios dominios con canalizaciones con barras verticales (|). El primer dominio se utiliza como una cadena para etiquetar los archivos que están protegidos por las aplicaciones que utilizan WIP. Por ejemplo, `example.com|example.net`.

Windows 10: configuración de perfil de Windows Information Protection	Descripción
Archivo de certificado de recuperación de datos (.der, .cer)	Esta configuración especifica el archivo de certificado de recuperación de datos. El archivo que especifique debe contar con un certificado codificado mediante PEM o DER con una extensión de archivo .der o .cer. Utilice el archivo de certificado de recuperación de datos para recuperar archivos que estaban protegidos localmente en un dispositivo. Por ejemplo, si su empresa desea recuperar datos protegidos por WIP de un dispositivo. Para obtener información sobre un certificado de recuperación de datos, consulte la documentación de Microsoft Windows Information Protection.
Eliminar la configuración de Windows Information Protection cuando se elimine un dispositivo de BlackBerry UEM	Esta configuración especifica si se revoca la configuración WIP cuando se desactiva un dispositivo. Cuando se revoca la configuración de WIP, el usuario ya no puede acceder a los archivos protegidos.
Mostrar superposiciones de Windows Information Protection en aplicaciones y archivos protegidos que pueden crear contenidos de la empresa	Esta configuración especifica si se muestra un icono superpuesto en los archivos y los iconos de aplicaciones para indicar si un archivo o aplicación está protegido por WIP.
Rango IP de la red de trabajo	Esta configuración especifica el intervalo de direcciones IP en el trabajo con las que puede compartir datos una aplicación protegida con WIP. Utilice un guión para indicar un rango de direcciones. Utilice una coma para separar las direcciones.
Los intervalos de IP de red de trabajo son autoritativos	Esta configuración especifica si solo se aceptan los intervalos IP de la red de trabajo como parte de la red de trabajo. Cuando se activa esta opción, no se realizan intentos para descubrir otras redes de trabajo. De manera predeterminada, la opción no está seleccionada.
Servidores de proxy internos de la empresa	Esta configuración especifica los servidores proxy internos que se utilizan cuando se conecta a ubicaciones de la red de trabajo. Estos servidores proxy solo se utilizan cuando se conecta al dominio enumerado en la configuración de recursos de la nube de la empresa.
Recursos en la nube de la empresa	En la configuración se especifica la lista de dominios de recursos de empresa alojados en la nube que se deben proteger. Los datos de estos recursos se consideran los datos de la empresa y se protegen.
Dominio de recursos en la nube	En la configuración se especifica el nombre de dominio.

Windows 10: configuración de perfil de Windows Information Protection	Descripción
Proxy emparejado	En la configuración se especifica un proxy que está emparejado con un recurso en la nube. El tráfico al recurso de nube se enrutará a través de la red empresarial mediante el servidor proxy denotado (en el puerto 80). También se debe configurar un servidor proxy para este propósito en el campo Servidores de proxy internos de la empresa.
Servidores proxy de la empresa	Esta configuración especifica la lista de servidores proxy de internet.
Los servidores proxy de la empresa son autoritativos	Esta configuración especifica si el cliente debe aceptar la lista configurada de servidores proxy y no intentar detectar otros proxy de empresa.
Recursos neutrales	En la configuración se especifican los dominios que desea que se puedan utilizar para recursos de trabajo o personales.
Nombres de dominio de la red de la empresa	Esta configuración especifica una lista de dominios separada por comas que abarca los límites de la empresa. Los datos procedentes de uno de dichos dominios que se envíen a un dispositivo se considerarán datos de la empresa y estarán protegidos. Estas ubicaciones se considerarán destinos seguros para compartir los datos de la empresa. Por ejemplo, `example.com`, `example.net`.

Windows 10: configuración de perfil de Windows Information Protection	Descripción

Código de carga de las aplicaciones de escritorio	Especifique las claves de las aplicaciones de escritorio y los valores utilizados para configurar las restricciones de inicio de las aplicaciones en los dispositivos Windows 10. Debe utilizar las claves definidas por Microsoft para el tipo de carga que desea configurar.
	
	Para especificar las aplicaciones, copie el código XML del archivo .xml de la política AppLocker y péguelo en este campo. Cuando copie el texto, copie únicamente los elementos como se muestran en el ejemplo de código siguiente.
	
	`<RuleCollection Type="Appx" EnforcementMode="Enabled">`
	`<FilePublisherRule Id="0c9781aa-bf9f-4352-b4ba-64c25f36f558"`
	`Name="WordMobile" Description=""`
	`UserOrGroupSid="S-1-1-0" Action="Allow">`
	`<Conditions>`
	`<FilePublisherCondition`
	`PublisherName="CN=Microsoft Corporation, O=Microsoft Corporation,`
	`L=Redmond, S=Washington, C=US"`
	`ProductName="Microsoft.Office.Word" BinaryName="*">`
	`<BinaryVersionRange LowSection="*" HighSection="*" />`
	`</FilePublisherCondition>`
	`</Conditions>`
	`</FilePublisherRule>`
	`</RuleCollection>`
	
	Para obtener más información sobre el uso de AppLocker, consulte la documentación de Microsoft AppLocker.

Windows 10: configuración de perfil de Windows Information Protection	Descripción

Código de carga de las aplicaciones de Universal Windows Platform	Especifique las claves y los valores de las aplicaciones de Universal Windows Platform utilizados para configurar WIP en dispositivos Windows 10. Debe utilizar las claves definidas por Microsoft para el tipo de carga que desea configurar.
	
	Para especificar las aplicaciones, copie el código XML del archivo .xml de la política AppLocker y péguelo en este campo. Cuando copie el texto, copie únicamente los elementos como se muestran en el ejemplo de código siguiente.
	
	`<RuleCollection Type="Exe" EnforcementMode="Enabled">`
	`<FilePathRule`
	`Id="921cc481-6e17-4653-8f75-050b80acca20" Name="(Default Rule)`
	`All files"`
	`Description="" UserOrGroupSid="S-1-1-0" Action="Allow">`
	`<Conditions>`
	
	`<FilePathCondition Path="*" />`
	`</Conditions>`
	`</FilePathRule>`
	
	`<FilePublisherRule Id="ddd0bc90-dada-4002-9e2f-0fc68e1f6af0" Name="WORDPAD.EXE,`
	`from O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US"`
	`Description=""`
	
	`UserOrGroupSid="S-1-1-0" Action="Deny">`
	
	`<Conditions>`
	
	`<FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION,`
	
	`L=REDMOND, S=WASHINGTON, C=US" ProductName="*" BinaryName="WORDPAD.EXE">`
	
	`<BinaryVersionRange LowSection="*" HighSection="*" />`
	`</FilePublisherCondition>`
	`</Conditions>`
	`</FilePublisherRule>`
	
	`<FilePublisherRule Id="c8360d06-f651-4883-abdd-9c3a95a415ff" Name="NOTEPAD.EXE,`
	`from O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US"`
	`Description=""`
	
	`UserOrGroupSid="S-1-1-0" Action="Allow">`
	
	`<Conditions>`
	
	`<FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION,`
	
	`L=REDMOND, S=WASHINGTON, C=US" ProductName="*" BinaryName="NOTEPAD.EXE">`

Windows 10: configuración de perfil de Windows Information Protection	Descripción
Perfil VPN asociado	Esta configuración especifica el perfil VPN que un dispositivo utiliza para conectarse a una red VPN cuando utiliza una aplicación protegida por WIP. Esta configuración solo es válida si está seleccionado "Utilizar un perfil de VPN" para "Conexión segura utilizada con WIP".
Recopilar registros de auditoría del dispositivo	En la configuración se especifica si desea recopilar registros de auditoría del dispositivo.

Configuración del perfil de protección de aplicaciones de Microsoft Intune

Los perfiles de protección de aplicaciones de Microsoft Intune son compatibles con los siguientes tipos de dispositivos:

- iOS
- Android

Común: configuración del perfil de protección de aplicaciones de Microsoft Intune

Configuración del perfil de protección de aplicaciones de Intune	Descripción
Interoperabilidad	
Activar interoperabilidad entre las aplicaciones Intune y Dynamics	Esta configuración especifica si las aplicaciones de BlackBerry Dynamics pueden interactuar con aplicaciones gestionadas por Intune como aplicaciones de Microsoft Office 365 en el dispositivo. Para permitir la interoperabilidad entre las aplicaciones de BlackBerry Dynamics y las aplicaciones gestionadas por Intune, se debe instalar BlackBerry Enterprise BRIDGE en los dispositivos de los usuarios. Para obtener más información, consulte la Guía de administración de BlackBerry Enterprise BRIDGE
Reubicación de datos	

Configuración del perfil de protección de aplicaciones de Intune	Descripción
Interoperabilidad	
Permitir a las aplicaciones transferir datos a otras aplicaciones	En la configuración se especifican las aplicaciones a las que pueden mandar datos las aplicaciones Intune gestionadas. Valores posibles: • Aplicaciones gestionadas por políticas: esta opción le permite transferir datos solo a otras aplicaciones gestionadas por Intune. • Todas las aplicaciones • Ninguno
Permitir a las aplicaciones recibir datos de otras aplicaciones	En la configuración se especifican las aplicaciones que pueden recibir datos de las aplicaciones gestionadas por la directiva de protección de aplicaciones. Valores posibles: • Aplicaciones gestionadas por políticas: esta opción le permite transferir datos solo desde otras aplicaciones gestionadas por Intune. • Todas las aplicaciones • Ninguno
Impedir "Guardar como"	En la configuración se especifica si desea activar la opción "Guardar como" para las aplicaciones. Si selecciona esta configuración, puede permitir el uso de la opción "Guardar como" para guardar los datos de trabajo solo en una o más de las ubicaciones siguientes: • Almacenamiento local • OneDrive for Business • SharePoint
Restringir cortar, copiar y pegar con otras aplicaciones	En la configuración se especifica cómo pueden utilizarse las operaciones de cortar, copiar y pegar con la aplicación. Valores posibles: • Bloqueado: esta opción impide las operaciones de cortar, copiar y pegar entre la aplicación y otras aplicaciones. • Aplicaciones gestionadas por políticas: esta opción permite las operaciones de cortar, copiar y pegar entre la aplicación y otras aplicaciones que se gestionan por Intune. • Aplicaciones gestionadas por políticas con pegar: esta opción permite pegar los datos desde cualquier aplicación, pero los datos cortados o copiados desde una aplicación gestionada por políticas se pueden pegar únicamente a otras aplicaciones gestionadas por Intune. • Cualquier aplicación: esta opción permite operaciones de cortar, copiar y pegar entre todas las aplicaciones del dispositivo.

Configuración del perfil de protección de aplicaciones de Intune	Descripción
Interoperabilidad	
Restringir contenido web para mostrar en Managed Browser	En la configuración se especifica si los enlaces web en aplicaciones deben abrirse en un navegador gestionado por Intune.
Desactivar sincronización de contactos	Esta configuración especifica si desea que la aplicación pueda guardar contactos en la aplicación Contactos nativa del dispositivo.
Desactivar impresión	Esta configuración especifica si desea que la aplicación pueda imprimir datos.
Acceder	
Requerir credenciales corporativas para el acceso	En la configuración se especifica si los usuarios deben utilizar sus credenciales de la organización para acceder a la aplicación. Si esta regla está seleccionada, tendrá prioridad sobre los requisitos de PIN o huella digital.
Bloquear las aplicaciones gestionadas para que no se ejecuten en dispositivos con jailbreak o rooting	En la configuración se especifica si desea que se puedan ejecutar aplicaciones en dispositivos con jailbreak o rooting.
Volver a comprobar el periodo de tiempo de espera de los requisitos de acceso	En la configuración se especifica, en minutos, con qué frecuencia desea que se vuelvan a comprobar los requisitos de acceso de la aplicación cuando esta esté abierta.
Periodo de gracia sin conexión	En la configuración se especifica, en minutos, con qué frecuencia desea que se vuelvan a comprobar los requisitos de acceso del dispositivo cuando esté sin conexión.
Intervalo sin conexión antes de que se eliminen los datos de la aplicación	En la configuración se especifica, en días, cuánto tiempo puede estar desconectado un dispositivo antes de que se eliminen los datos de la aplicación.
Requerir PIN para acceder	En la configuración se especifica si los usuarios deben introducir un código PIN para acceder a la aplicación. Si esta opción está seleccionada, se pedirá al usuario que proporcione un código PIN la primera vez que ejecute la aplicación. Si está seleccionada la configuración "Requerir credenciales corporativas para el acceso", tendrá prioridad sobre esta regla.
Número de intentos antes del restablecimiento del PIN	Esta configuración especifica el número de veces que se puede intentar introducir el PIN antes de que el usuario tenga que restablecerlo.

Configuración del perfil de protección de aplicaciones de Intune	Descripción
Interoperabilidad	
Permitir PIN simple	Esta configuración especifica si los usuarios pueden utilizar secuencias de PIN simples como 1234 o 1111.
Longitud del PIN	Esta configuración especifica el número mínimo de dígitos del PIN.
Permitir huella digital en lugar de PIN	Esta configuración especifica si los usuarios pueden utilizar una huella dactilar en lugar de un código PIN para acceder a la aplicación. Esta configuración es compatible con iOS 8.0 y posteriores y 6.0 Android y posteriores.
Desactivar PIN de aplicación cuando el PIN del dispositivo está gestionado	En esta configuración se especifica si la aplicación solicita el PIN cuando el dispositivo debe tener una contraseña. Si se selecciona esta configuración, el PIN de la aplicación no se solicita en dispositivos Android si la política de TI UEM del dispositivo requiere una contraseña. Para desactivar el PIN de la aplicación en dispositivos iOS, Intune debe requerir el PIN del dispositivo.

iOS: configuración del perfil de protección de aplicaciones de Microsoft Intune

Configuración del perfil de protección de aplicaciones de Intune	Descripción
Cifrar datos de la aplicación	En la configuración se especifica cuándo los datos de las aplicaciones están cifrados. Valores posibles: • Si el dispositivo está bloqueado: esta opción cifra todos los datos de la aplicación cuando el dispositivo está bloqueado. • Si el dispositivo está bloqueado y los archivos abiertos: esta opción cifra todos los datos de la aplicación cuando el dispositivo está bloqueado. Los datos de los archivos abiertos no están cifrados • Después de reiniciar el dispositivo: esta opción cifra los datos de las aplicaciones cuando se reinicia el dispositivo hasta que el dispositivo se encuentra desbloqueado por primera vez. • Utilizar la configuración del dispositivo: esta opción cifra los datos de las aplicaciones según la configuración predeterminada del dispositivo. Esta opción requiere que los usuarios definan una contraseña en el dispositivo.
Impedir copias de seguridad de iTunes y iCloud	En la configuración se especifica si se puede realizar una copia de seguridad de iTunes o iCloud.

Configuración del perfil de protección de aplicaciones de Intune	Descripción
Identificadores de paquete de la aplicación	En la configuración se especifican los ID de paquete de las aplicaciones a las que se aplica este perfil. Puede introducir el ID del paquete o seleccionar en la lista de aplicaciones gestionadas por Intune disponibles.
Requerir sistema operativo iOS mínimo	Seleccione esta opción para especificar una versión de iOS mínima para poder utilizar esta aplicación. Si la versión de iOS que está instalada en el dispositivo no cumple este requisito, el usuario no podrá utilizar la aplicación. Se puede especificar un decimal (por ejemplo, 10.3).
Requerir sistema operativo iOS mínimo (solo advertencia)	Seleccione esta opción para especificar una versión de iOS mínima recomendada para poder utilizar esta aplicación. Si la versión de iOS que está instalada en el dispositivo no cumple este requisito, el usuario recibirá una notificación que no se podrá descartar. Se puede especificar un decimal (por ejemplo, 10.3).
Requerir versión de aplicación mínima	Seleccione esta opción para especificar una versión de aplicación mínima para poder utilizar esta aplicación. Si la versión de la aplicación que está instalada en el dispositivo no cumple este requisito, el usuario no podrá utilizar la aplicación. Se puede especificar un decimal (por ejemplo, 4.2). Debido a que diferentes aplicaciones suelen tener esquemas de versión distintas, si quiere especificar una versión de aplicación mínima, debe crear un perfil separada para cada aplicación.
Requerir versión de aplicación mínima (solo advertencia)	Seleccione esta opción para especificar una versión de aplicación mínima recomendada para poder utilizar esta aplicación. Si la versión de la aplicación que está instalada en el dispositivo no cumple este requisito, el usuario recibirá una notificación que no se podrá descartar. Se puede especificar un decimal (por ejemplo, 4.2). Debido a que diferentes aplicaciones suelen tener esquemas de versión distintas, si quiere especificar una versión de aplicación mínima, debe crear un perfil separada para cada aplicación.

Android: configuración del perfil de protección de aplicaciones de Microsoft Intune

Configuración del perfil de protección de aplicaciones de Intune	Descripción
Cifrar datos de la aplicación	En la configuración se especifica si los datos de las aplicaciones están cifrados. Si selecciona esta regla, los datos de la aplicación se cifrarán de forma sincrónica durante todas las tareas de entrada y salida de archivos.
Evitar las copias de seguridad de Android	En la configuración se especifica si se puede realizar una copia de seguridad de los datos de la aplicación a Android Backup Service.

Configuración del perfil de protección de aplicaciones de Intune	Descripción
Bloquear captura de pantalla y Android Assistant	En la configuración se especifica si la captura de pantalla y las capacidades de escaneo de la aplicación Android Assistant están permitidas cuando se utiliza una aplicación protegida. Esta configuración es compatible con Android 6.0 o posteriores.
Identificadores de paquete de la aplicación	En la configuración se especifican los ID de paquete de las aplicaciones a las que se aplica este perfil. Puede introducir el ID del paquete o seleccionar en la lista de aplicaciones gestionadas por Intune disponibles.
Requerir versión de Android mínima	Seleccione esta opción para especificar una versión de Android mínima para poder utilizar esta aplicación. Si la versión de Android que está instalada en el dispositivo no cumple este requisito, el usuario no podrá utilizar la aplicación. Puede especificar hasta cuatro identificadores de versión. Separe los identificadores de versión con puntos (por ejemplo, 10.3 o 10.3.14.2).
Requerir versión mínima de Android (solo advertencia)	Seleccione esta opción para especificar una versión de Android mínima recomendada para poder utilizar esta aplicación. Si la versión de Android que está instalada en el dispositivo no cumple este requisito, el usuario recibirá una notificación que no se podrá descartar. Puede especificar hasta cuatro identificadores de versión. Separe los identificadores de versión con puntos (por ejemplo, 10.3 o 10.3.14.2).
Requerir versión mínima de parche de Android	Seleccione esta opción para especificar una versión mínima de parche de Android para poder utilizar esta aplicación. Si la versión del parche de Android que está instalada en el dispositivo no cumple este requisito, el usuario no podrá utilizar la aplicación. Especifique la versión con el formato de fecha AAAA-MM-DD.
Requerir versión mínima de parche de Android (solo advertencia)	Seleccione esta opción para especificar una versión mínima de parche de Android recomendada para poder utilizar esta aplicación. Si la versión del parche de Android que está instalada en el dispositivo no cumple este requisito, el usuario recibirá una notificación que se puede descartar. Especifique la versión con el formato de fecha AAAA-MM-DD.
Requerir versión de aplicación mínima	Seleccione esta opción para especificar una versión de aplicación mínima para poder utilizar esta aplicación. Si la versión de la aplicación que está instalada en el dispositivo no cumple este requisito, el usuario no podrá utilizar la aplicación. Puede especificar hasta cuatro identificadores de versión. Separe los identificadores de versión con puntos (por ejemplo, 10.3 o 10.3.14.2). Debido a que diferentes aplicaciones suelen tener esquemas de versión distintas, si quiere especificar una versión de aplicación mínima, debe crear un perfil separada para cada aplicación.

Configuración del perfil de protección de aplicaciones de Intune	Descripción
Requerir versión de aplicación mínima (solo advertencia)	Seleccione esta opción para especificar una versión de aplicación mínima recomendada para poder utilizar esta aplicación. Si la versión de la aplicación que está instalada en el dispositivo no cumple este requisito, el usuario recibirá una notificación que no se podrá descartar. Puede especificar hasta cuatro identificadores de versión. Separe los identificadores de versión con puntos (por ejemplo, 10.3 o 10.3.14.2). Debido a que diferentes aplicaciones suelen tener esquemas de versión distintas, si quiere especificar una versión de aplicación mínima, debe crear un perfil separada para cada aplicación.

Hoja de cálculo de referencia de políticas

Para obtener más información acerca de las políticas de TI, descargue la hoja de cálculo de referencia de políticas en help.blackberry.com/detectLang/blackberry-uem/current/policy-reference-spreadsheet-zip/.

Glosario

AES	Advanced Encryption Standard (Estándar de cifrado avanzado)
AET	identificador de inscripción de la aplicación
APN	Servicio Apple Push Notification
BES5	BlackBerry Enterprise Server 5
BES10	BlackBerry Enterprise Service 10
BES12	BlackBerry Enterprise Service 12
Instancia de BES12	Una instancia de BES12 se refiere a todos los componentes de BES12 instalados en un ordenador excepto BlackBerry Router, que es un componente opcional que se instala por separado. Una instancia de BES12 se denomina en ocasiones como "unidad de escala".
protocolo entre procesos de BlackBerry	El protocolo entre procesos de BlackBerry es un protocolo propio de BlackBerry que genera la clave de sesión que los componentes de BlackBerry Enterprise Solution, como BlackBerry Enterprise Server y BlackBerry Mobile Voice System, pueden utilizar para comunicarse de una forma muy segura entre sí. El protocolo entre procesos de BlackBerry genera la clave de sesión basada en la contraseña de comunicación.
BlackBerry UEM domain	A BlackBerry UEM domain consists of a BlackBerry UEM database and a BlackBerry Control database and any BlackBerry UEM instances that connect to them.
BlackBerry UEM instance	A BlackBerry UEM instance refers to one installation of the BlackBerry UEM Core and all associated BlackBerry UEM components that communicate with it. The components can be installed on the same server or multiple servers. There can be more than one BlackBerry UEM instance in a BlackBerry UEM domain.
CA	autoridad del certificado
certificado	Un certificado es un documento digital que vincula la identidad y la clave pública del sujeto de un certificado. Cada certificado tiene una clave privada correspondiente que se almacena por separado. Una

	autoridad del certificado firma el certificado para indicar que es auténtico y de confianza.
CRL	lista de revocación de certificados
DEP	Programa de inscripción de dispositivos de
DNS	Domain Name System (Sistema de nombres de dominio)
DPD	Detección de punto muerto
EAP	Extensible Authentication Protocol (Protocolo de autenticación extensible)
EAP-FAST	Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling (Protocolo de autenticación extensible - Autenticación flexible mediante túnel seguro)
EAP-MS-CHAP	Extensible Authentication Protocol Microsoft Challenge Handshake Authentication Protocol (Protocolo de autenticación extensible - Protocolo de autenticación por desafío mutuo de Microsoft)
EAP-TLS	Extensible Authentication Protocol - Transport Layer Security (Protocolo de autenticación extensible - Seguridad de la capa de transporte)
EDP	enterprise data protection
EMM	Enterprise Mobility Management (Gestión de movilidad empresarial)
FQDN	Fully Qualified Domain Name (Nombre de dominio completo)
GTC	Tarjeta del identificador genérico
HMAC	Keyed-Hash Message Authentication Code (Código de autenticación de mensaje de hash en clave)
HTTP	Hypertext Transfer Protocol (Protocolo de transferencia de hipertexto)
HTTPS	Hypertext Transfer Protocol over Secure Sockets Layer (Protocolo de transferencia de hipertexto a través de un nivel de socket seguro)
ICCID	Integrated Circuit Card Identifier (Identificador de tarjeta de circuito integrado)

IKE	Internet Key Exchange (Intercambio de claves de Internet)
IMAP	Internet Message Access Protocol (Protocolo de acceso a mensajes de Internet)
IMEI	International Mobile Equipment Identity (Identidad internacional de equipos móviles)
IP	Internet Protocol (Protocolo de Internet)
IPsec	Internet Protocol Security (Seguridad del protocolo de Internet)
Política de TI	Una política de TI consiste en varias reglas que controlan las características de seguridad y el comportamiento de los dispositivos.
LAN	Local Area Network (Red de área local)
LDAP	Lightweight Directory Access Protocol (Protocolo ligero de acceso a directorios)
MD5	Algoritmo Message-Digest, versión 5
MDM	Gestión de dispositivos móviles
MS-CHAP	Microsoft Challenge Handshake Authentication Protocol (Protocolo de autenticación por desafío mutuo de Microsoft)
NAT	traducción de dirección de red
NTLM	Personal Information Management (Gestor de LAN NT)
OCSP	Online Certificate Status Protocol (Protocolo de estado de certificados en línea)
OID	identificador de objeto
PAC	proxy auto-configuration (configuración automática del proxy)
PFS	Confidencialidad directa total
PKI	Public Key Infrastructure (Infraestructura de claves públicas)
PMK	pairwise master key (clave principal por pares)
POP	Post Office Protocol (Protocolo de oficina de correos)

PRF	familia de función pseudoaleatoria
PSK	pre-shared key (clave previamente compartida)
SCEP	Simple certificate enrollment protocol (Protocolo simple de inscripción de certificados)
SHA	Secure Hash Algorithm (Algoritmo de hash seguro)
SIM	Subscriber Identity Module (Módulo de identidad del abonado)
S/MIME	Secure Multipurpose Internet Mail Extensions (Extensiones seguras multiuso del correo de Internet)
SNMP	Simple Network Management Protocol (Protocolo simple de administración de red)
espacio	Un espacio es un área específica del dispositivo que permite la clasificación y administración de los distintos tipos de datos, aplicaciones y conexiones de red. Los distintos espacios pueden tener distintas reglas para el almacenamiento de datos, permisos de aplicaciones y enrutamiento de red. Los espacios se denominaban antes "perímetros".
SSL	Secure Sockets Layer (Capa de sockets seguros)
Dispositivos iOS supervisados	Los dispositivos supervisados están configurados para permitir un control adicional de las características de los dispositivos iOS. Para activar la supervisión de los dispositivos iOS que pertenecen a la empresa, puede usar Apple Configurator o el Programa de inscripción de dispositivos.
TCP	Transmission Control Protocol (Protocolo de control de transmisión)
TGT	El Vale de concesión de vales (TGT) es un vale de servicio que el cliente de un servicio habilitado para Kerberos envía al TGS para solicitar el vale de servicio para dicho servicio habilitado para Kerberos.
TLS	Transport Layer Security (Seguridad de capa de transporte)
UEM	Gestión unificada de extremos
USB	Bus de serie universal (Universal Serial Bus)
VPN	virtual private network (red privada virtual)
xAuth	Autenticación ampliada

Aviso legal

©2019 BlackBerry Limited. BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, MOVIRTU y SECUSMART, entre otras, son marcas comerciales o marcas registradas de BlackBerry Limited, de sus subsidiarias o filiales, sujetas a licencia, cuyos derechos exclusivos están expresamente reservados. El resto de marcas comerciales pertenecen a sus respectivos propietarios.

GOOD y EMBLEM Design son marcas comerciales o marcas comerciales registradas de BlackBerry Limited, de sus subsidiarias o filiales, sujetas a licencia, cuyos derechos exclusivos están expresamente reservados.

Android, Google Chrome y Google Play son marcas comerciales de Google Inc. Apple, App Store, Apple Configurator, iCloud, macOS, y Safari son marcas comerciales de Apple Inc. Aruba y VIA son marcas comerciales de Aruba Networks, Inc. Bell es una marca comercial de Bell Canada. Blue Coat es una marca comercial de Blue Coat Systems, Inc. Bluetooth es una marca comercial de Bluetooth SIG. Check Point y VPN-1 son marcas comerciales de Check Point Software Technologies Ltd. Cisco, Cisco AnyConnect, Cisco IOS, y PIX son marcas comerciales de Cisco Systems, Inc. o de sus filiales en los Estados Unidos y en otros países. F5 es una marca comercial de F5 Networks, Inc. HTC EVO es una marca comercial de HTC Corporation. IBM, Domino, IBM Verse, y Notes son marcas comerciales de International Business Machines Corporation, registradas en muchas jurisdicciones de todo el mundo. iOS es una marca comercial de Cisco Systems, Inc. o de sus filiales en EE. UU. y otros países. iOS® se usa bajo licencia de Apple Inc. Juniper es una marca comercial de Juniper Networks, Inc. Kerberos es una marca comercial de Massachusetts Institute of Technology. Microsoft, Active Directory, ActiveSync, Azure, Windows, y Windows Phone son marcas comerciales registradas o marcas comerciales de Microsoft Corporation en Estados Unidos y/o en otros países. OpenSSL es una marca comercial de The OpenSSL Software Foundation, Inc. OpenVPN es una marca comercial de OpenVPN Technologies, Inc. OpenTrust y OpenTrust CMS son marcas comerciales de Docusign France société par actions simplifiée (sas). PGP es una marca comercial de PGP Corporation. Pulse Secure es una marca comercial de Pulse Secure LLC. QR Code es una marca comercial de DENSO WAVE1 INCORPORATED en Japón y en otros países. RSA es una marca comercial de RSA Security. SonicWALL y Mobile Connect son marcas comerciales de Dell, Inc. Symantec es una marca comercial o marca comercial registrada de Symantec Corporation o de sus filiales en Estados Unidos. y otros países. T-Mobile es una marca comercial de Deutsche Telekom AG. Wi-Fi, WPA, y WPA2 son marcas comerciales de Wi-Fi Alliance. Entrust, Entrust IdentityGuard, y Entrust Authority Administration Services son marcas comerciales de Entrust, Inc. KNOX y Samsung KNOX son marcas comerciales de Samsung Electronics Co., Ltd. Vuzix M300 Smart Glasses es una marca comercial de Vuzix Corporation. El resto de marcas comerciales pertenecen a sus respectivos propietarios.

Esta documentación, incluida cualquier documentación que se incorpore mediante referencia como documento proporcionado o disponible en el sitio web de BlackBerry, se proporciona o se pone a disposición "TAL CUAL" y "SEGÚN SU DISPONIBILIDAD" sin ninguna condición, responsabilidad ni garantía de ningún tipo por parte de BlackBerry Limited y sus empresas afiliadas ("BlackBerry"), y BlackBerry 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 BlackBerry, así como los secretos comerciales, la presente documentación describe algunos aspectos de la tecnología de BlackBerry en líneas generales. BlackBerry 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"). BlackBerry no controla ni es responsable de ningún tipo de Productos y servicios de terceros, lo que incluye, sin restricciones, el contenido, la exactitud, el cumplimiento de copyright, la compatibilidad, el rendimiento, la fiabilidad, 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 BlackBerry se haga responsable de dichos Productos y servicios de terceros ni 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. ASIMISMO, PODRÍA DISPONER DE OTROS DERECHOS QUE VARÍAN SEGÚN EL ESTADO O LA PROVINCIA. ES POSIBLE QUE ALGUNAS JURISDICCIONES NO PERMITAN LA EXCLUSIÓN O LA LIMITACIÓN DE GARANTÍAS Y CONDICIONES IMPLÍCITAS. 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 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 BLACKBERRY ASUMIRÁ RESPONSABILIDAD ALGUNA POR CUALQUIER TIPO DE DAÑOS RELACIONADOS CON ESTA DOCUMENTACIÓN O SU USO, O POR EL 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 DAÑO 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 BLACKBERRY, COSTES DEBIDOS AL TIEMPO DE INACTIVIDAD, PÉRDIDA DE USO DE LOS PRODUCTOS Y SERVICIOS DE BLACKBERRY O PARTE DE ELLOS 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 COMO SI NO, Y AUNQUE SE HAYA AVISADO A BLACKBERRY DE LA POSIBILIDAD DE DICHOS DAÑOS.

EN LA MEDIDA MÁXIMA EN QUE LO PERMITA LA LEY DE SU JURISDICCIÓN, BLACKBERRY 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 POR SU PARTE, INCLUIDA PERO NO LIMITADA AL INCUMPLIMIENTO DEL CONTRATO, NEGLIGENCIA, AGRAVIO, 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 BLACKBERRY Y A SUS EMPRESAS AFILIADAS, SUS SUCESORES, CESIONARIOS, AGENTES, PROVEEDORES (INCLUIDOS LOS PROVEEDORES DE SERVICIOS DE USO), DISTRIBUIDORES AUTORIZADOS POR BLACKBERRY (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 BLACKBERRY O CUALQUIER AFILIADO DE BLACKBERRY 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. Es posible que algunos proveedores de servicios de uso no ofrezcan la función de exploración de Internet con una suscripción a 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 Productos y servicios de

terceros con productos y servicios de BlackBerry pueden precisar la obtención de una o más patentes, marcas comerciales, derechos de autor u otras licencias para evitar que se vulneren o infrinjan 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 BlackBerry se le facilita para su comodidad "TAL CUAL" sin ninguna condición expresa e implícita, aprobación, garantía de cualquier tipo por BlackBerry, y BlackBerry no asume ninguna responsabilidad en relación con ellos. El uso de los Productos y servicios de terceros estará sujeto a la aceptación de los términos de las licencias independientes aplicables en este caso con terceros, excepto en los casos cubiertos expresamente por una licencia u otro acuerdo con BlackBerry.

Los términos de uso de cualquier producto o servicio de BlackBerry se presentan en una licencia independiente o en otro acuerdo con BlackBerry aplicable según corresponda. NADA DE LO DISPUESTO EN LA PRESENTE DOCUMENTACIÓN SUSTITUIRÁ NINGÚN ACUERDO EXPRESO POR ESCRITO NI NINGUNA GARANTÍA QUE PROPORCIONE BLACKBERRY PARA PARTES DE CUALQUIER PRODUCTO O SERVICIO DE BLACKBERRY QUE NO SEA ESTA DOCUMENTACIÓN.

BlackBerry Enterprise Software incluye software de terceros. La información de licencia y copyright asociada a este software está disponible en http://worldwide.blackberry.com/legal/thirdpartysoftware.jsp.

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

BlackBerry UK Limited
200 Bath Road
Slough, Berkshire SL1 3XE
Reino Unido

Publicado en Canadá