BlackBerry UEM

Configuración

12.16

Contents

Configuración de BlackBerry UEM por primera vez..... 7
Permisos de administrador requeridos para configurar BlackBerry UEM..... 8
Adquisición y activación de licencias..... 8

Cambio de certificados de BlackBerry UEM..... 9
Consideraciones para cambiar los certificados de BlackBerry Dynamics..... 10
Cambio de un certificado de BlackBerry UEM..... 11

Configuración de BlackBerry UEM para enviar datos a través de un servidor proxy..... 13
Envío de datos a través de un servidor proxy TCP a BlackBerry Infrastructure..... 13
Comparación de los servidores proxy TCP..... 14
Configuración de BlackBerry UEM para utilizar un servidor proxy TCP transparente..... 14
Activación de SOCKS v5 en un servidor proxy TCP..... 15
Envío de datos a través de BlackBerry Router a BlackBerry Infrastructure..... 15
Configuración de BlackBerry UEM para utilizar BlackBerry Router..... 15

Configuración de conexiones mediante los servidores proxy internos..... 17
Configuración de los ajustes de proxy del lado del servidor..... 17

Conexión con los directorios de la empresa..... 18
Configuración de la autenticación de Microsoft Active Directory en un entorno que incluya buzones de correo vinculados a Exchange..... 18
Conexión a una instancia de Microsoft Active Directory..... 19
Conexión a un directorio LDAP..... 20
Permitir los grupos vinculados al directorio..... 22
Permitir integración..... 23
Activación y configuración de la integración y la extracción..... 24
Sincronización de una conexión de directorio de empresa..... 25
Vista previa del informe de sincronización..... 25
Visualización de un informe de sincronización..... 25
Agregar un programa de sincronización..... 25
Eliminación de una conexión a un directorio de la empresa..... 27

Conexión a un servidor SMTP para enviar notificaciones de correo..... 28
Conexión a un servidor SMTP para enviar notificaciones de correo..... 28

Configuración de replicación de bases de datos..... 29
Pasos para configurar la replicación de la base de datos..... 29
Requisitos previos: Configuración de replicación de bases de datos..... 29

Creación y configuración de la base de datos replicada....30
Conexión de BlackBerry UEM con la base de datos replicada....30
Configuración de una nueva base de datos replicada....31

Conexión de BlackBerry UEM a Microsoft Azure.... 32
Crea una cuenta de Microsoft Azure.... 32
Sincronización de Microsoft Active Directory con Microsoft Azure.... 33
Creación de un extremo empresarial en Azure.... 33
Configuración del acceso condicional de Azure Active Directory....34
Configuración de acceso condicional de Azure Active Directory.... 35
Quitar dispositivos del acceso condicional de Azure Active Directory....36

Permiso de acceso a BlackBerry Web Services mediante BlackBerry Infrastructure....37

Adquisición de certificado APN para gestionar los dispositivos iOS y macOS.. 38
Obtener una CSR firmada de BlackBerry.... 38
Solicitud de un certificado APN de Apple....39
Registro del certificado APN....39
Renovación del certificado APN.... 39
Solución de problemas de APN....40
El certificado APN no coincide con la CSR. Proporcione el archivo APN (.pem) correcto o envíe una nueva CSR....40
Se muestra el mensaje "El sistema ha detectado un error" cuando intento obtener una CSR firmada....40
No puedo activar dispositivos con iOS o macOS.... 40

Configuración de BlackBerry UEM para DEP.... 42
Creación de una cuenta de DEP....42
Descarga de una clave pública....42
Generación de un identificador del servidor....43
Registro del identificador del servidor con BlackBerry UEM.... 43
Adición de la configuración de la primera inscripción....43
Actualización del identificador del servidor....45
Eliminar conexión de DEP.... 45

Configuración de BlackBerry UEM para que admita dispositivos Android Enterprise.... 47
Configuración de BlackBerry UEM para admitir dispositivos Android Enterprise.... 48
Eliminación de la conexión con el dominio de Google....49
Eliminación de la conexión de dominio de Google con su cuenta de Google....50
Edición o prueba de la conexión de dominio de Google.... 50

Simplificación de activaciones de Windows 10.... 51
Integración de UEM con la combinación Azure Active Directory....51
Integración de UEM con la combinación de Azure Active Directory.... 52

Configuración de Windows Autopilot en Microsoft Azure....53
Creación de un perfil de implementación de Windows Autopilot en Azure 53
Importación de dispositivos Windows Autopilot a Azure....53
Implementación de un servicio de detección para simplificar las activaciones Windows 10....54

Migración de usuarios, dispositivos, grupos y otros datos desde un servidor de origen....57

Requisitos previos: Migración de usuarios, dispositivos, grupos y otros datos desde un servidor de origen....57
Conexión con un servidor de origen....59
Exportación del certificado raíz autofirmado para el servidor de Good Control....61
Consideraciones: migración de políticas de TI, perfiles y grupos desde un servidor de origen....62
Migración de políticas de TI, perfiles y grupos desde un servidor de origen....64
Complete la migración de políticas y perfiles para los usuarios activados para BlackBerry Dynamics....64
Funciones de Good Control en BlackBerry UEM....65
Consideraciones: Migración de usuarios desde un servidor de origen....67
Migración de usuarios desde un servidor de origen....68
Consideraciones: migración de dispositivos desde un servidor de origen....68
Referencia rápida de migración de dispositivos....72
Migración de dispositivos desde un servidor de origen....73
Migración de dispositivos DEP....74
Migración de dispositivos DEP que tienen BlackBerry UEM Client instalado....74
Migre los dispositivos DEP que no tengan BlackBerry UEM Client instalado y no tengan activado BlackBerry Dynamics....74

Configuración de BlackBerry UEM para admitir las aplicaciones de BlackBerry Dynamics....75

Gestión de clústeres de BlackBerry Proxy....75
Configuración de Direct Connect utilizando reenvío de puertos....76
Configuración de las propiedades de BlackBerry Dynamics....77
Propiedades globales de BlackBerry Dynamics....77
Propiedades de BlackBerry Dynamics....81
Propiedades de BlackBerry Proxy....82
Configuración de los parámetros de comunicación de las aplicaciones de BlackBerry Dynamics....84
Envío de los datos de aplicaciones de BlackBerry Dynamics a través de un proxy HTTP....84
Consideraciones del archivo PAC 84
Configuración de los ajustes de proxy de la aplicación BlackBerry Dynamics....85
Conectividad y comportamiento de enrutamiento de BlackBerry Dynamics....86
Ruta predeterminada....86
Ejemplos de escenarios de enrutamiento....88
Flujo de datos de BlackBerry Dynamics....91
Configuración de Kerberos para aplicaciones de BlackBerry Dynamics....92
Dominios, dominios Kerberos y bosques....92
Requisitos previos....94
Configuración de la delegación restringida Kerberos....94
Resolución de problemas y diagnósticos....97
Configuración de Kerberos PKINIT....97
Conexión de BlackBerry UEM a un conector PKI de BlackBerry Dynamics....98

Integración de BlackBerry UEM con Cisco ISE....100

Requisitos: integración de BlackBerry UEM con Cisco ISE..... 100
Creación de una cuenta de administrador que Cisco ISE pueda utilizar..... 101
Adición del certificado de BlackBerry Web Services al almacén de certificados de Cisco ISE..... 102
Conexión de BlackBerry UEM a Cisco ISE..... 102
Ejemplo: Reglas de políticas de autorización para BlackBerry UEM..... 103
Administración del acceso a la red y de los controles del dispositivo con Cisco ISE..... 104
Redirección de los dispositivos que no están activados en BlackBerry UEM..... 106

Aviso legal..... 107

Configuración de BlackBerry UEM por primera vez

La siguiente tabla muestra un resumen de las tareas de configuración inicial incluidas en esta guía. Utilice esta tabla para determinar qué tareas de configuración se deberían completar. Cuando haya completado las tareas correspondientes, podrá configurar administradores, crear y administrar usuarios y grupos, configurar los controles del dispositivo y activar dispositivos.

Tarea	Descripción
Sustitución de los certificados predeterminados por certificados de confianza	Puede reemplazar los certificados autofirmados predeterminados utilizados por BlackBerry UEM para autenticar la comunicación entre varios componentes y dispositivos de UEM.
Configuración de BlackBerry UEM para enviar datos a través de un servidor proxy	Puede configurar BlackBerry UEM para enviar datos a través de un servidor proxy TCP o una instancia de BlackBerry Router antes de que lleguen a BlackBerry Infrastructure. También puede configurar BlackBerry UEM para enviar datos a través de un proxy HTTP antes de que lleguen a BlackBerry Dynamics NOC.
Configuración de conexiones a través de servidores de proxy internos	Si su empresa utiliza un servidor proxy para las conexiones entre servidores dentro de la red, es posible que tenga que configurar los ajustes de proxy del lado del servidor para permitir a BlackBerry UEM Core comunicarse con las instancias remotas de la consola de gestión.
Conexión de BlackBerry UEM a los directorios de la empresa	Puede conectar BlackBerry UEM a uno o más directorios de la empresa, como Microsoft Active Directory o un directorio LDAP, de forma que BlackBerry UEM pueda acceder a los datos del usuario para crear cuentas de usuario.
Conexión de BlackBerry UEM a un servidor SMTP	Si desea que BlackBerry UEM envíe mensajes de correo de activación y otras notificaciones a los usuarios, debe especificar la configuración del servidor SMTP que BlackBerry UEM puede utilizar.
Configuración de la replicación de la base de datos	Para conservar el servicio de la base de datos y la integridad de los datos si ocurren problemas con la base de datos de BlackBerry UEM, puede instalar y configurar una base de datos de conmutación por error que sirva de copia de seguridad de la base de datos principal.
Conexión de BlackBerry UEM a Microsoft Azure	Si desea utilizar BlackBerry UEM para implementar aplicaciones de iOS y Android gestionadas por Microsoft Intune o si desea administrar aplicaciones de Windows 10 en BlackBerry UEM, conecte BlackBerry UEM a Microsoft Azure.
Adquisición y registro de un certificado APN	Si desea gestionar y enviar datos a dispositivos iOS o macOS, debe obtener una CSR firmada de BlackBerry, utilizarla para obtener un certificado APN de Apple y registrar el certificado APN con el dominio de BlackBerry UEM.
Configuración de BlackBerry UEM para el programa de inscripción de dispositivos Apple	Si desea utilizar la consola de gestión de BlackBerry UEM para gestionar dispositivos iOS que su empresa adquirió de Apple para DEP, debe configurar esta función.

Tarea	Descripción
Configuración de BlackBerry UEM para admitir dispositivos Android Enterprise	Para admitir dispositivos Android Enterprise, tiene que configurar el dominio de G Suite o de Google Cloud para que sea compatible con los proveedores de gestión de dispositivos móviles de terceros y configurar BlackBerry UEM para comunicarse con el dominio de G Suite o de Google Cloud.
Configuración de la red para simplificar las activaciones de Windows 10	Puede simplificar el proceso de activación de dispositivos Windows 10 mediante la realización de cambios en la configuración de la red para que los usuarios no tengan que escribir una dirección de servidor.
Migración de usuarios, dispositivos, grupos y otros datos desde un servidor de origen	Puede utilizar la consola de gestión para migrar usuarios, dispositivos, grupos y otros datos desde una base de datos local de origen de BlackBerry UEM o Good Control (independiente).
Configuración de BlackBerry Dynamics	Puede configurar las opciones específicas de las aplicaciones de BlackBerry Proxy y BlackBerry Dynamics.
Integración de BlackBerry UEM con Cisco ISE	Puede crear una conexión entre Cisco ISE y BlackBerry UEM para que Cisco ISE pueda recuperar los datos del dispositivo desde BlackBerry UEM y ejecutar las políticas de control de acceso a la red.

Permisos de administrador requeridos para configurar BlackBerry UEM

Al realizar las tareas de configuración de esta guía, inicie sesión en la consola de gestión mediante la cuenta de administrador que ha creado al instalar BlackBerry UEM. Si desea que más de una persona complete las tareas de configuración, puede crear cuentas de administrador adicionales. Para obtener más información acerca de la creación de cuentas de administrador, consulte el contenido referente a Administración.

Si crea cuentas de administrador adicionales para configurar BlackBerry UEM, debería asignar la función de administrador de seguridad a dichas cuentas. La función de administrador de seguridad predeterminada tiene los permisos necesarios para completar cualquier tarea de configuración.

Adquisición y activación de licencias

Para poder activar dispositivos se deben obtener las licencias necesarias. Las licencias deben obtenerse antes de seguir las instrucciones de configuración que se describen en esta guía y antes de agregar las cuentas de usuario.

Para obtener más información acerca de las opciones de licencia y las funciones y productos que admiten los diferentes tipos de licencia, consulte el contenido referente a Licencias.

Cambio de certificados de BlackBerry UEM

Cuando se instala BlackBerry UEM, la aplicación de configuración genera varios certificados autofirmados que se utilizan para autenticar la comunicación entre distintos componentes de UEM y los dispositivos. Puede cambiar los certificados si la política de seguridad de su empresa requiere que los certificados los firme la autoridad de certificación de su empresa o si desea utilizar certificados emitidos por una autoridad de certificación que ya son de confianza para los dispositivos y navegadores.

Nota: Si se producen problemas al cambiar un certificado, la comunicación entre los componentes de UEM y entre UEM y los dispositivos puede verse interrumpida. Si decide cambiar los certificados, planifique y pruebe el cambio con cuidado.

Puede cambiar los siguientes certificados:

Certificado	Descripción
Certificado SSL para consolas	Un certificado SSL que la consola de gestión de BlackBerry UEM y BlackBerry UEM Self-Service utilizan para autenticar los navegadores. Si configura la alta disponibilidad, el certificado debe tener el nombre del dominio de BlackBerry UEM. Puede encontrar el nombre de dominio de BlackBerry UEM en la consola de gestión en Configuración > Infraestructura > Instancias.
Certificados SSL para BlackBerry Web Services	Un certificado SSL que BlackBerry Web Services utiliza para autenticar las aplicaciones que utilizan las API de BlackBerry Web Services para gestionar BlackBerry UEM. Si configura la alta disponibilidad, el certificado debe tener el nombre del dominio de BlackBerry UEM. Puede encontrar el nombre de dominio de BlackBerry UEM en la consola de gestión en Configuración > Infraestructura > Instancias.
Certificado de firma de perfil de Apple	Un certificado que BlackBerry UEM utiliza para firmar el perfil de MDM que los usuarios deben aceptar cuando activan dispositivos iOS. Si está utilizando un certificado firmado por una CA, asegúrese de que el certificado raíz de la CA está instalado en los dispositivos iOS de los usuarios antes de la activación.
Certificado SSL para aplicaciones BlackBerry Dynamics	Un certificado SSL que BlackBerry Dynamics Launcher utiliza para establecer un canal de comunicación seguro con BlackBerry UEM. Las aplicaciones de BlackBerry Dynamics que integran BlackBerry Dynamics Launcher pueden presentar el certificado a BlackBerry UEM para autenticarse en el servidor.
Certificado para servidores de BlackBerry Dynamics	Un certificado SSL que autentica las conexiones entre BlackBerry UEM y BlackBerry Proxy.

Certificado	Descripción
Certificado de gestión de aplicaciones	Un certificado SSL que se utiliza para a autenticación entre las aplicaciones de BlackBerry UEM y BlackBerry Dynamics. El certificado de CA raíz de este certificado se almacena en la lista de certificados de CA de confianza en el dispositivo. Cuando el servidor se autentica en el dispositivo, presenta este certificado al dispositivo para su validación. Si cambia este certificado y el cambio se hace efectivo antes de que BlackBerry UEM inserte el certificado en todas las aplicaciones BlackBerry Dynamics, será necesario volver a activar las aplicaciones que no hayan recibido el certificado.
Certificado para Direct Connect	Certificado SSL que se utiliza para la autenticación entre un servidor de BlackBerry Proxy configurado para BlackBerry Dynamics Direct Connect y aplicaciones BlackBerry Dynamics en los dispositivos del usuario final. Al actualizar este certificado, la nueva versión siempre se enviará a los dispositivos a través de una conexión que no es de BlackBerry Dynamics Direct Connect. En los dispositivos o contenedores que no estén en línea en el momento del cambio se aplicará la actualización cuando vuelvan a estar en línea. La actualización de este certificado debe realizarse al mismo tiempo en el servidor de BlackBerry UEM y en cualquier dispositivo de red aplicable. Para obtener más información acerca de la configuración de Direct Connect, consulte Configuración de Direct Connect con BlackBerry UEM

Consideraciones para cambiar los certificados de BlackBerry Dynamics

Si desea cambiar cualquiera de los certificados SSL de BlackBerry Dynamics, tenga en cuenta las consideraciones siguientes. Si se producen problemas al cambiar un certificado, la comunicación entre los componentes de BlackBerry UEM y entre las aplicaciones de BlackBerry UEM y BlackBerry Dynamics podría verse interrumpida. Planifique y pruebe los cambios de certificados con cuidado.

Adición de nuevos certificados a cualquier equipo periférico

Si ha agregado certificados de BlackBerry Dynamics a equipos periféricos de su red, agregue el nuevo certificado al equipo periférico antes de agregarlo a BlackBerry UEM.

Actualización de las aplicaciones de BlackBerry Dynamics

Si va a sustituir el certificado de BlackBerry Dynamics para la administración de aplicaciones o Direct Connect, asegúrese de que las aplicaciones de BlackBerry Dynamics de los usuarios se actualizan a las versiones más recientes antes de sustituir el certificado.

Las de BlackBerry Dynamics aplicaciones desarrolladas por su empresa deben contar con la versión 3.2 o posterior del SDK de BlackBerry Dynamics. Las aplicaciones más antiguas no pueden recibir el nuevo certificado de BlackBerry UEM.

Las aplicaciones de BlackBerry Dynamics debe estar abiertas para recibir un certificado

Los usuarios deben abrir una aplicación de BlackBerry Dynamics para que reciba un certificado de BlackBerry UEM. Si va a sustituir el certificado de BlackBerry Dynamics para la administración de aplicaciones o Direct Connect y el cambio se hace efectivo antes de que BlackBerry UEM inserte el certificado en todas las aplicaciones de BlackBerry Dynamics, será necesario volver a activar las aplicaciones que no hayan recibido el certificado. Las aplicaciones no reciben certificados mientras están suspendidas en dispositivos iOS o mientras los dispositivos Android están en modo Descanso.

Asegúrese de que BlackBerry Connectivity Node está accesible

Si cualquiera de las instancias de BlackBerry Proxy no está accesible para BlackBerry UEM cuando se sustituyen los certificados de BlackBerry Dynamics, las aplicaciones de BlackBerry Dynamics no podrán conectarse a esas instancias después de la sustitución de los certificados.

Programe los cambios de certificados de forma adecuada

Si va a sustituir el certificado para servidores de BlackBerry Dynamics, elija un periodo de baja actividad para reiniciar los servidores.

Deje un tiempo suficiente para que los nuevos certificados se propaguen a las aplicaciones de BlackBerry Proxy y BlackBerry Dynamics. Si va a sustituir solo el certificado de los servidores de BlackBerry Dynamics, deje al menos 10 minutos para que se reinicie el servidor.

Si va a sustituir el certificado de BlackBerry Dynamics para la administración de aplicaciones o Direct Connect, es recomendable que el tiempo hasta la fecha efectiva sea más largo que la configuración de "Última hora de contacto" de verificación de la conectividad en el perfil de cumplimiento.

Si va a sustituir tanto los certificados de BlackBerry Dynamics para la administración de aplicaciones como para Direct Connect, establezca las horas efectivas con una separación mínima de 30 minutos. Si tiene un gran número de usuarios y aplicaciones de BlackBerry Dynamics, debe esperar más de 30 minutos entre cada certificado.

Cambio de un certificado de BlackBerry UEM

Antes de empezar:

- Obtenga un certificado firmado por una CA de confianza. El certificado debe estar en un formato de almacén de claves (.pfx, .pkcs12).
- Si va a sustituir el certificado de BlackBerry Dynamics para la administración de aplicaciones o Direct Connect, asegúrese de que las aplicaciones de BlackBerry Dynamics de los usuarios se actualizan a las versiones más recientes en primer lugar.

1. En la barra de menús, haga clic en **Configuración > Infraestructura > Certificados de servidor**.
2. En la sección del certificado que vaya a sustituir, haga clic en **Ver detalles**.
3. Haga clic en **Sustituir certificado**.
4. Navegue hasta el archivo de certificado y selecciónelo.
5. Introduzca una contraseña de cifrado para el certificado.
6. Si va a sustituir un certificado para servidores de BlackBerry Dynamics, especifique cuándo desea que se reinicie BlackBerry UEM para que el cambio surta efecto.

   Es recomendable que elija un periodo de baja actividad para reiniciar los servidores.

7. Si va a sustituir el certificado de BlackBerry Dynamics para la administración de aplicaciones o Direct Connect, especifique la fecha efectiva para el cambio de certificado.

   Es recomendable que la fecha efectiva esté alejada de la configuración de "Última hora de contacto" de verificación de la conectividad en el perfil de cumplimiento. Si va a cambiar más de un certificado, debe separar las horas efectivas al menos 30 minutos entre sí. Tenga en cuenta que no se solicita la fecha de efectiva cuando el nuevo certificado lo emite la misma CA que el certificado anterior. Para obtener más información, visite support.blackberry.com/community para leer el artículo 74167.
8. Haga clic en **Sustituir**.

Después de terminar:

- Si ha sustituido alguno de los certificados de la pestaña **Certificados de servidor**, reinicie el servicio BlackBerry UEM Core en todos los servidores. Es recomendable que elija un periodo de baja actividad para reiniciar los servidores.
- En el caso de los certificados de la pestaña Certificados de BlackBerry Dynamics, puede hacer clic en **Revertir al valor predeterminado** para volver a utilizar un certificado autofirmado.
- En la pestaña Certificados de BlackBerry Dynamics, puede desactivar las casillas de verificación **Confiar en la CA de BlackBerry UEM** y **Confiar en la CA de BlackBerry Dynamics** si ya no necesita certificados autofirmados. Puede desactivar la casilla de verificación **Confiar en la CA de BlackBerry Dynamics** solo si ha sustituido todos los certificados en la pestaña Certificados de BlackBerry Dynamics.
- Si las aplicaciones de BlackBerry Dynamics dejan de comunicarse después de cambiar los certificados, asegúrese de que las aplicaciones están actualizadas y, a continuación, indique a los usuarios que vuelvan a activarlas.

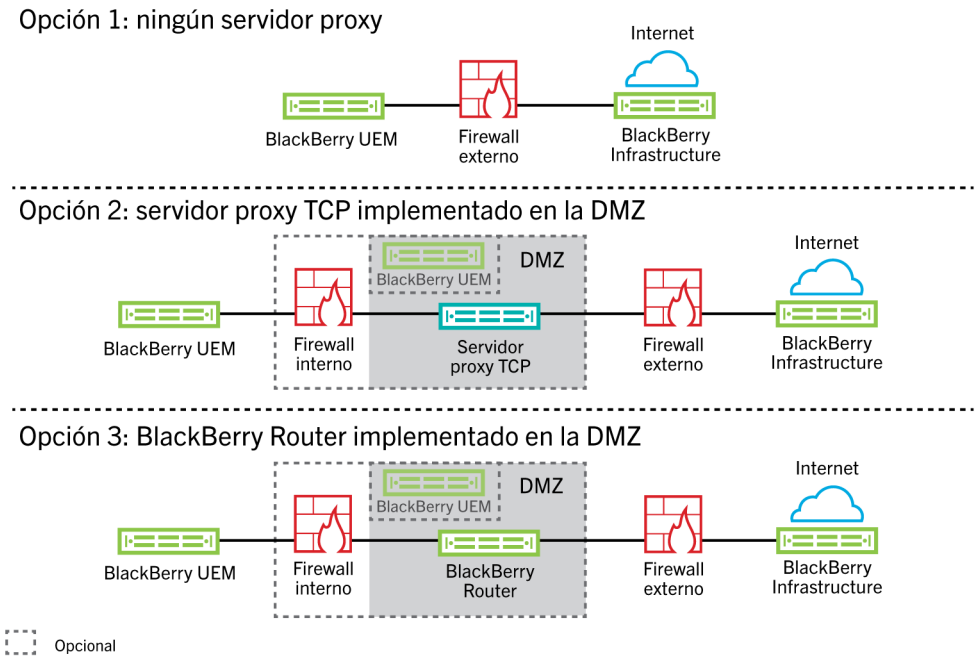
Configuración de BlackBerry UEM para enviar datos a través de un servidor proxy

Puede configurar BlackBerry UEM para enviar datos a través de un servidor proxy TCP o una instancia de BlackBerry Router antes de que lleguen a BlackBerry Infrastructure.

De forma predeterminada, BlackBerry UEM se conecta directamente a BlackBerry Infrastructure mediante el puerto 3101. Si la política de seguridad de la empresa requiere que los sistemas internos no puedan conectarse directamente a Internet, puede instalar BlackBerry Router o un servidor proxy TCP. BlackBerry Router o el servidor proxy TCP actúan como un intermediario entre BlackBerry UEM y BlackBerry Infrastructure.

Puede instalar BlackBerry Router o un servidor proxy fuera del firewall de la empresa en una DMZ. La instalación de BlackBerry Router o de un servidor proxy TCP en una DMZ proporciona un nivel adicional de seguridad para BlackBerry UEM. Solo BlackBerry Router o el servidor proxy se conectan a BlackBerry UEM desde fuera del firewall. Todas las conexiones a BlackBerry Infrastructure entre BlackBerry UEM y los dispositivos se realizan a través de BlackBerry Router o el servidor proxy.

Esta imagen muestra las siguientes opciones para enviar datos a través de un servidor proxy a BlackBerry Infrastructure: ningún servidor proxy, un servidor proxy TCP implementado en una DMZ y BlackBerry Router implementado en una DMZ.



Envío de datos a través de un servidor proxy TCP a BlackBerry Infrastructure

Puede configurar un servidor proxy TCP transparente para el servicio de BlackBerry UEM Core y otro para el servicio de BlackBerry Affinity Manager. Estos servicios requieren una conexión saliente y también pueden tener diferentes puertos configurados. No se pueden instalar o configurar varios servidores proxy TCP transparentes para cada servicio.

Se pueden configurar varios servidores proxy TCP configurados con SOCKS v5 (sin autenticación) para conectarse a BlackBerry UEM. Varios servidores proxy TCP configurados con SOCKS v5 (sin autenticación) pueden proporcionar apoyo si una de las instancias de servidor proxy activo no está funcionando correctamente.

Puede configurar un solo puerto que todas las instancias de servicio SOCKS v5 deben escuchar. Si desea configurar más de un servidor proxy TCP con SOCKS v5, cada servidor debe compartir el puerto de escucha del proxy.

Comparación de los servidores proxy TCP

Proxy	Descripción
Proxy TCP transparente	• Intercepta la comunicación normal en la capa de red sin requerir ninguna configuración de cliente especial • No requiere una configuración del navegador cliente • Generalmente se ubica entre el cliente e internet • Realiza algunas de las funciones de una puerta de enlace o un router • Se utiliza a menudo para aplicar la política de uso aceptable • Comúnmente los ISP lo utilizan en algunos países para ahorrar ancho de banda de subida y mejorar los tiempos de respuesta al cliente a través del almacenamiento en caché
Proxy SOCKS v5	• Es un protocolo de internet para manejar el tráfico de internet a través de un servidor proxy • Se puede controlar con prácticamente cualquier aplicación TCP/UDP, incluidos navegadores y clientes FTP compatibles con SOCKS • Puede ser una buena solución para el anonimato en internet y la seguridad • Enruta los paquetes de red entre un cliente y el servidor a través de un servidor proxy • Puede proporcionar la autenticación de modo que solo los usuarios autorizados puedan tener acceso a un servidor • Conexiones de servidores proxy TCP con una dirección IP arbitraria • Puede anonimizar los protocolos UDP y TCP como HTTP

Configuración de BlackBerry UEM para utilizar un servidor proxy TCP transparente

Antes de empezar: Instale un servidor proxy TCP transparente compatible en el dominio de BlackBerry UEM.

1. En la barra de menús, haga clic en **Configuración > Infraestructura > BlackBerry Router y proxy**.
2. Seleccione la opción **Servidor proxy**.
3. Lleve a cabo cualquiera de las tareas siguientes:

Tarea	Pasos
Enrute los datos TCP a través de un servidor proxy TCP.	En los campos **BlackBerry UEM Core y BlackBerry Secure Gateway Service**, escriba el FQDN o la dirección IP y el número de puerto del servidor proxy. Cada campo requiere un valor único.
Enrute el tráfico SRP a través de un servidor proxy TCP.	En el campo **Affinity Manager**, escriba el FQDN o la dirección IP y el número de puerto del servidor proxy. Cada campo requiere un valor único.

Tarea	Pasos
Enrute el tráfico de BlackBerry Secure Connect Plus a través de un servidor proxy TCP.	En los campos **BlackBerry Secure Connect Plus**, introduzca el FQDN o la dirección IP y el número de puerto del servidor proxy. Cada campo requiere un valor único.

4. Haga clic en **Guardar**.

Activación de SOCKS v5 en un servidor proxy TCP

Antes de empezar: Instale un servidor proxy TCP compatible con SOCKS v5 (sin autenticación) en el dominio de BlackBerry UEM.

1. En la barra de menús, haga clic en **Configuración > Infraestructura > BlackBerry Router y proxy**
2. Seleccione la opción **Servidor proxy**.
3. Seleccione la casilla de verificación **Activar SOCKS v5**.
4. Haga clic en +.
5. En el campo **Dirección del servidor**, escriba la dirección IP o el nombre de host del servidor proxy SOCKS v5.
6. Haga clic en **Agregar**.
7. Repita los pasos 1 a 6 para cada servidor proxy SOCKS v5 que desea configurar.
8. En el campo **Puerto**, escriba el número de puerto.
9. Haga clic en **Guardar**.

Envío de datos a través de BlackBerry Router a BlackBerry Infrastructure

Puede configurar varias instancias de BlackBerry Router para conseguir una alta disponibilidad. Puede configurar un solo puerto para que las instancias de BlackBerry Router escuchen.

BlackBerry UEM no es compatible con una instancia de BlackBerry Router utilizada originalmente con BES5.

De forma predeterminada, BlackBerry UEM se conecta a BlackBerry Router mediante el puerto 3102 para los servicios BlackBerry UEM y el puerto 3101 para los servicios BES5. BlackBerry Router es compatible con todo el tráfico de salida de BlackBerry UEM Core y BlackBerry Affinity Manager.

Nota: Si desea utilizar un puerto diferente al puerto predeterminado para BlackBerry Router, visite support.blackberry.com/community y lea el artículo 36385.

Configuración de BlackBerry UEM para utilizar BlackBerry Router

Antes de empezar: Instale BlackBerry Router en el dominio de BlackBerry UEM. Para obtener instrucciones sobre la instalación de BlackBerry Router, consulte el contenido referente a Instalación y actualización.

1. En la barra de menús, haga clic en **Configuración > Infraestructura > BlackBerry Router y proxy**.
2. Seleccione la opción **BlackBerry Router**.
3. Haga clic en +.
4. Escriba la dirección IP o el nombre de host de la instancia de BlackBerry Router que desee conectar a BlackBerry UEM.
5. Haga clic en **Agregar**.

6. Repita los pasos 1 a 5 para cada instancia de BlackBerry Router que desee configurar.
7. En el campo **Puerto**, escriba el número de puerto que todas las instancias de BlackBerry Router escuchan. El valor predeterminado es 3102.
8. Haga clic en **Guardar**.

Configuración de conexiones mediante los servidores proxy internos

Si su empresa utiliza un servidor proxy para las conexiones entre servidores dentro de la red, es posible que tenga que configurar los ajustes de proxy del lado del servidor para permitir a BlackBerry UEM Core comunicarse con la consola de gestión de BlackBerry UEM si está instalada en un equipo independiente. Asimismo, deberá configurar los ajustes de proxy del lado del servidor para permitir a BlackBerry UEM comunicarse con otros servicios internos, como las autoridades de certificación y los servidores que alojan aplicaciones de notificación para enviar datos al BlackBerry MDS Connection Service.

Los ajustes de proxy del lado del servidor no se aplican a las conexiones salientes. Para obtener información sobre la configuración de BlackBerry UEM para utilizar un servidor proxy TCP, consulte Configuración de BlackBerry UEM para enviar datos a través de un servidor proxy.

Configuración de los ajustes de proxy del lado del servidor

Antes de empezar: Asegúrese de que tiene la URL de PAC o el nombre de host y el número de puerto, así como otros ajustes que necesite para conectar con el servidor proxy.

1. En la barra de menús, haga clic en **Configuración > Infraestructura > Proxy del lado del servidor**.
2. Si la mayoría o la totalidad de los servidores que forman parte de su instalación de BlackBerry UEM deben conectarse a un servidor proxy, realice las acciones siguientes para definir la configuración global del proxy del lado del servidor.
   a) En **Opciones de proxy globales del lado del servidor**, en la lista **Tipo**, seleccione **Configuración de PAC** o **Configuración manual**
   b) Especifique la configuración que necesite el servidor proxy y haga clic en **Guardar**.
3. Si uno o varios de los servidores requieren una configuración de proxy distinta de la global, realice las acciones siguientes para definir la configuración de proxy del servidor:
   a) En el nombre del servidor, en la lista **Tipo**, seleccione **Ninguno**, **Configuración de PAC** o **Configuración manual**.
   b) Si ha seleccionado **Configuración de PAC** o **Configuración manual**, especifique la configuración que necesita el servidor proxy.
   c) Haga clic en **Guardar**.

Conexión con los directorios de la empresa

Puede conectar BlackBerry UEM al directorio de la empresa para que pueda tener acceso a la lista de usuarios de su empresa. Puede conectar BlackBerry UEM a varios directorios y los directorios pueden ser una combinación de Microsoft Active Directory y LDAP.

Cuando el directorio de la empresa está conectado, puede aprovechar las ventajas de las siguientes funciones:

- Puede crear cuentas de usuario en BlackBerry UEM mediante el uso de datos del usuario del directorio y BlackBerry UEM puede autenticar a los administradores para la consola de gestión y los usuarios para BlackBerry UEM Self-Service.
- Puede vincular los grupos de directorios de la empresa con grupos de BlackBerry UEM para organizar a los usuarios en BlackBerry UEM de la misma forma que se organizan en el directorio de su empresa. Consulte Permitir los grupos vinculados al directorio.
- Puede activar la integración para grupos específicos en el directorio de la empresa para crear usuarios de BlackBerry UEM automáticamente. Si activa la integración, también puede configurar la extracción para eliminar datos de dispositivos o cuentas de usuario cuando los usuarios se eliminan de los grupos en el directorio de su empresa. Consulte Permitir integración.

Si no se puede conectar BlackBerry UEM a un directorio de la empresa, puede crear manualmente las cuentas de usuario locales y autenticar a los administradores mediante la autenticación predeterminada.

Para conectar BlackBerry UEM a un directorio de la empresa, realice las siguientes acciones:

Paso	Acción
1	Crear una conexión a una instancia de Microsoft Active Directory o a un directorio LDAP. Si su entorno incluye un bosque de recursos, consulte Configuración de la autenticación de Microsoft Active Directory en un entorno que incluya buzones de correo vinculados a Exchange.
2	De forma opcional, activar los grupos vinculados a directorios.
3	De forma opcional, activar la integración.
4	De forma opcional, agregar un programa de sincronización.

Configuración de la autenticación de Microsoft Active Directory en un entorno que incluya buzones de correo vinculados a Exchange

En un modelo de bosque de recursos, el servidor de Microsoft Exchange se encuentra en un bosque (el bosque de recursos) y las cuentas de usuario individuales se encuentran en bosques de cuentas. Si el entorno de la empresa incluye un bosque de recursos que se dedica a la ejecución de Microsoft Exchange, puede configurar la autenticación de Microsoft Active Directory para cuentas de usuario que se encuentren ubicadas en bosques de cuentas de confianza.

Si hay un bosque de recursos de Exchange en el entorno de la empresa, debe configurar BlackBerry UEM para conectarse al bosque de recursos. Debe crear un buzón de correo en el bosque de recursos para cada cuenta de usuario y, a continuación, asociar estos buzones de correo con las cuentas de usuario. Al asociar los buzones de correo del bosque de recursos con cuentas de usuario de los bosques de cuentas, las cuentas de usuario obtienen acceso total a los buzones de correo y las cuentas de usuario de los bosques de cuentas se conectan al servidor de Microsoft Exchange. BlackBerry UEM utiliza los buzones de correo para buscar las cuentas de usuario en los distintos dominios.

Para autenticar los usuarios que inician sesión en BlackBerry UEM, BlackBerry UEM debe leer la información de usuario que se guarda en los servidores de catálogo global que forman parte del bosque de recursos. Debe crear una cuenta de Microsoft Active Directory para BlackBerry UEM que se encuentre en un dominio de Windows que forme parte del bosque de recursos. Al crear la conexión de directorio, proporcione el dominio de Windows, el nombre de usuario y la contraseña de la cuenta de Microsoft Active Directory y, en caso de que sea necesario, los nombres de los servidores de catálogo global que BlackBerry UEM puede utilizar.

Para obtener más información, visite technet.microsoft.com y lea *Administrar buzones vinculados*.

Conexión a una instancia de Microsoft Active Directory

Antes de empezar: Cree una cuenta de Microsoft Active Directory que BlackBerry UEM pueda utilizar. La cuenta debe cumplir los siguientes requisitos:

- Debe estar ubicada en un dominio de Windows que sea parte del bosque de Microsoft Exchange.
- Debe tener permiso para acceder a los contenedores de usuario y leer los objetos de usuario guardados en los servidores de catálogo global en el bosque de Microsoft Exchange.
- La contraseña debe configurarse para que no caduque y no necesita cambiarse en el siguiente inicio de sesión.
- Si activa el inicio de sesión único, debe configurar la delegación restringida de la cuenta.
- El servidor de UEM también debe estar vinculado con el dominio de Active Directory.

1. En la barra de menús, haga clic en **Configuración > Integración externa > Directorio de la empresa**.
2. Haga clic en **Agregar una conexión de Microsoft Active Directory**.
3. En el campo **Nombre de la conexión de directorio**, escriba un nombre para la conexión de directorio.
4. En el campo **Nombre de usuario**, escriba el nombre de usuario de la cuenta de Microsoft Active Directory.
5. En el campo **Dominio**, escriba el nombre del dominio de Windows que forma parte del bosque de Microsoft Exchange en formato DNS (por ejemplo, ejemplo.com).
6. En el campo **Contraseña**, escriba la contraseña de la cuenta.
7. En la lista desplegable **Selección del centro de distribución de claves Kerberos**, lleve a cabo una de las siguientes acciones:
   - Para permitir que BlackBerry UEM detecte automáticamente los centros de distribución de claves (KDC), haga clic en **Automático**.
   - Para especificar la lista de KDC de BlackBerry UEM que debe utilizarse para la autenticación, haga clic en **Manual**. En el campo **Nombres de servidor**, escriba el nombre del controlador de dominio KDC en formato DNS (por ejemplo, kdc01.ejemplo.com). De forma opcional, puede incluir el número de puerto que utiliza el controlador de dominio (por ejemplo, kdc01.ejemplo.com:88). Haga clic en + para especificar qué controladores de dominio KDC adicionales desea que BlackBerry UEM utilice.
8. En la lista desplegable **Selección de catálogo global**, lleve a cabo una de las acciones siguientes:
   - Si desea que BlackBerry UEM detecte automáticamente los servidores de catálogo global, haga clic en **Automático**.

- Para especificar la lista de servidores de catálogo global que BlackBerry UEM utiliza, haga clic en **Manual.** En el campo **Nombres de servidor**, escriba el nombre de DNS del servidor de catálogo global al que desea que BlackBerry UEM acceda (por ejemplo, catálogoglobal01.ejemplo.com). De forma opcional, puede incluir el número de puerto que utiliza el servidor de catálogo global (por ejemplo, catálogoglobal01.com:3268). Haga clic en + para especificar servidores adicionales.

9. Haga clic en **Continuar**.
10. En el campo **Base de búsqueda del catálogo global**, realice una de las siguientes acciones:
    - Para permitir a BlackBerry UEM buscar en el catálogo global, deje el campo en blanco.
    - Para controlar qué cuentas de usuario pueden autenticar BlackBerry UEM, escriba el nombre distintivo del contenedor Usuario (por ejemplo, OU=sales,DC=example,DC=com).
11. Si desea activar la compatibilidad para grupos globales, en la lista desplegable **Compatibilidad con grupos globales**, haga clic en **Sí**.

    Si desea utilizar grupos globales para la integración, debe seleccionar **Sí**. Para configurar un dominio de grupo global, en la sección **Lista de dominios de grupo global**, haga clic en +. En el campo **Dominio**, seleccione el dominio que desee agregar. La selección predeterminada para el campo **¿Especificar nombre de usuario y contraseña?** es No. Si mantiene esta selección predeterminada, se utilizará el nombre de usuario y la contraseña de la conexión del bosque. Si selecciona Sí, debe proporcionar unas credenciales válidas para una cuenta de Microsoft Active Directory en el dominio que haya seleccionado. En el campo **Selección de KDC**, puede seleccionar Automático para permitir que BlackBerry UEM descubra automáticamente los centros de distribución de claves o Manual para especificar la lista de KDC que BlackBerry UEM utilizará para la autenticación. Haga clic en **Agregar**.
12. Si su entorno tiene un bosque de recursos de Microsoft Exchange, para activar la compatibilidad con los buzones de correo de Microsoft Exchange vinculados, en la lista desplegable **Compatibilidad con los buzones de Microsoft Exchange vinculados**, haga clic en **Sí**.

    Para configurar la cuenta de Microsoft Active Directory para cada bosque al que desea que BlackBerry UEM acceda, en la sección **Lista de bosques de cuentas**, haga clic en +. Especifique el nombre de dominio de usuario (el usuario puede pertenecer a cualquier dominio del bosque de cuentas), así como el nombre y la contraseña. Si es necesario, especifique los KDC que desea que BlackBerry UEM busque. Si es necesario, especifique los servidores de catálogo global a los que desea que BlackBerry UEM pueda acceder. Haga clic en **Agregar**.
13. Para activar el registro único, seleccione la casilla de verificación **Activar registro único de Windows**. Para obtener más información sobre el registro único, consulte el contenido de Administración. El registro único solo es compatible en un entorno local.
14. Para sincronizar más detalles de usuario desde el directorio de empresa, active la casilla de verificación **Sincronizar detalles adicionales del usuario**. Entre los detalles adicionales se incluyen el nombre de la empresa y el teléfono de la oficina.
15. Haga clic en **Guardar**.
16. Haga clic en **Cerrar**.

Después de terminar: Si desea agregar un programa de sincronización de directorios, consulte Agregar un programa de sincronización.

Conexión a un directorio LDAP

Antes de empezar:

- Cree una cuenta LDAP de BlackBerry UEM que se ubique en el directorio LDAP pertinente. La cuenta debe cumplir los siguientes requisitos:
  - La cuenta tiene permiso para leer todos los usuarios en el directorio.

- La contraseña de la cuenta no caduca nunca y no se requiere que el usuario cambie la contraseña en el siguiente inicio de sesión.

- Si la conexión LDAP cuenta con cifrado SSL, asegúrese de tener el certificado del servidor para la conexión LDAP y que el servidor LDAP admita TLS 1.2. Si se ha activado SSL, la conexión LDAP a BlackBerry UEM debe usar TLS 1.2.
- Compruebe los valores de atributo de LDAP que usa su empresa (en los pasos siguientes se ofrecen ejemplos para los valores de atributo típicos). Debe especificar los valores de atributo de LDAP a partir del paso 11.

1. En la barra de menús, haga clic en **Configuración > Integración externa > Directorio de la empresa**.
2. Haga clic en **Agregar una conexión LDAP**.
3. En el campo **Nombre de la conexión de directorio**, escriba un nombre para la conexión de directorio.
4. En la lista desplegable **Detección del servidor LDAP**, lleve a cabo una de las acciones siguientes:
   - Para detectar automáticamente el servidor LDAP, haga clic en **Automático**. En el campo **Nombre del dominio DNS**, escriba el nombre del dominio del servidor que aloja el directorio de la compañía.
   - Para especificar una lista de servidores LDAP, haga clic en **Seleccionar servidor de la lista a continuación**. En el campo **Servidor LDAP**, escriba el nombre del servidor LDAP. Para agregar más servidores LDAP, haga clic en +.
5. En la lista desplegable **Activar SSL**, lleve a cabo una de las siguientes acciones:
   - Si la conexión LDAP cuenta con cifrado SSL, haga clic en **Sí**. Junto al campo **Certificado SSL del servidor LDAP**, haga clic en **Examinar** y seleccione el certificado de servidor LDAP.
   - Si la conexión LDAP no cuenta con cifrado SSL, haga clic en **No**.
6. En el campo **Puerto LDAP**, escriba el número de puerto TCP para la comunicación. Los valores predeterminados son 636 para SSL activado o 389 para SSL desactivado.
7. En la lista desplegable **Autorización requerida**, lleve a cabo una de las siguientes acciones:
   - Si se requiere autorización para la conexión, haga clic en **Sí**. En el campo **Iniciar sesión**, escriba el DN del usuario autorizado para iniciar sesión en LDAP (por ejemplo, an=admin, o=Org1). En el campo **Contraseña**, escriba la contraseña.
   - Si no se requiere autorización para la conexión, haga clic en **No**.
8. En el campo **Base de búsqueda de usuario**, escriba el valor que desea utilizar como el DN de base para las búsquedas de información del usuario.
9. En el campo **Filtro de búsqueda LDAP de usuario**, escriba el filtro de búsqueda LDAP que se requiere para encontrar objetos de usuario en el servidor del directorio de la empresa. Por ejemplo, para IBM Domino Directory, escriba `(objectClass=Person)`.

   Nota: Si desea excluir las cuentas de usuario desactivadas de los resultados de búsqueda, escriba `(&(objectclass=user)(logindisabled=false))`.
10. En la lista desplegable **Ámbito de búsqueda de usuario de LDAP**, lleve a cabo una de las siguientes acciones:
    - Para buscar todos los objetos que siguen al objeto base, haga clic en **Todos los niveles**. Esta es la configuración predeterminada.
    - Para buscar objetos que están justo un nivel después del DN de base, haga clic en **Un nivel**.
11. En el campo **Identificador único**, escriba el nombre del atributo que identifica de forma única a cada usuario en el directorio LDAP de la empresa (debe ser una cadena invariable y exclusiva a nivel global). Por ejemplo, `dominoUNID` en IBM Domino LDAP 7 y posterior.
12. En el campo **Nombre**, introduzca el atributo del nombre de cada usuario (por ejemplo, `givenName`).
13. En el campo **Apellido**, introduzca el atributo del apellido de cada usuario (por ejemplo, `sn`).
14. En el campo **Atributo de inicio de sesión**, escriba el atributo de inicio de sesión que se utilizará para la autenticación (por ejemplo, `uid`).

15. En el campo **Dirección de correo**, escriba el atributo de la dirección de correo electrónico de cada usuario (por ejemplo, `mail`). Si no define el valor, se utilizará un valor predeterminado.
16. En el campo **Nombre para mostrar**, introduzca el atributo del nombre para mostrar de cada usuario (por ejemplo, `displayName`). Si no define el valor, se utilizará un valor predeterminado.
17. En el campo **Nombre de la cuenta de perfil de correo**, introduzca el atributo del nombre de la cuenta del perfil de correo de cada usuario (por ejemplo, `mail`).
18. En el campo **Nombre principal del usuario**, escriba el nombre principal del usuario para SCEP (por ejemplo, `mail`).
19. Para activar los grupos vinculados a directorios en la conexión de directorio, seleccione la casilla de verificación **Permitir los grupos vinculados a directorios**.

    Especifique la siguiente información:

    - En el campo **Base de búsqueda de grupos**, escriba el valor que desea utilizar como DN de base para las búsquedas de información de grupos.
    - En el campo **Filtro de búsqueda LDAP de grupos**, escriba el filtro de búsqueda LDAP que se requiere para encontrar objetos de grupos en el directorio de la empresa. Por ejemplo, para IBM Domino Directory, escriba `(objectClass=dominoGroup)`.
    - En el campo **Identificador exclusivo de grupo**, escriba el atributo del identificador exclusivo de cada grupo. Este atributo debe ser invariable y exclusivo globalmente (por ejemplo, `cn`).
    - En el campo **Nombre de grupo para mostrar**, escriba el atributo de cada nombre de grupo para mostrar (por ejemplo, `cn`).
    - En el campo **Atributo de pertenencia al grupo**, escriba el nombre del atributo de pertenencia al grupo. Los valores de atributo deben estar en formato DN (por ejemplo, `CN=jsmith,CN=Users,DC=example,DC=com`).
    - En el campo **Probar nombre de grupo#**, escriba el nombre de un grupo actual para validar los atributos de grupo especificados.
20. Haga clic en **Guardar**.
21. Haga clic en **Cerrar**.

Después de terminar: Si desea agregar un programa de sincronización de directorios, consulte Agregar un programa de sincronización.

Permitir los grupos vinculados al directorio

Antes de empezar: Verifique que una sincronización del directorio de la empresa no esté en curso. No puede guardar los cambios que realice en la conexión del directorio de la empresa hasta que se haya completado la sincronización.

1. En la barra de menús, haga clic en **Configuración > Integración externa > Directorio de la empresa**.
2. Haga clic en el nombre del directorio de la empresa que desea editar.
3. En la pestaña **Sincronizar configuración**, seleccione la casilla de verificación **Permitir los grupos vinculados a directorios**.
4. Para forzar la sincronización de los grupos de directorios de la empresa, seleccione la casilla de verificación **Forzar sincronización**.

   Si se selecciona, cuando un grupo se elimina del directorio de su empresa, los vínculos a ese grupo se eliminan de grupos vinculados a directorios y grupos de directorio de integración. Si todos los grupos de directorios de la empresa asociados a un grupo vinculado a directorios se eliminan, el grupo vinculado a directorios se convertirá en un grupo local. Si no se seleccionan, en caso de no encontrar un grupo de directorios de la empresa, el proceso de sincronización se cancela.

5. En el campo **Límite de sincronización**, escriba el número máximo de cambios que desea permitir para cada proceso de sincronización.

   La configuración predeterminada es cinco. Si el número de cambios que deben sincronizarse supera el límite de sincronización, puede impedir que se ejecute el proceso de sincronización. Los cambios se calculan sumando lo siguiente: los usuarios que se agregarán a los grupos, los usuarios que se eliminarán de los grupos, los usuarios que se van a integrar y los usuarios que se van a extraer.
6. En el campo **Nivel máximo de anidamiento de grupos de directorio**, escriba el número de niveles anidados para grupos de directorios de la empresa.
7. Haga clic en **Guardar**.

Después de terminar: Cree grupos vinculados a directorios. Para obtener más información, consulte el contenido de Administración.

Permitir integración

La integración permite agregar automáticamente las cuentas de usuario a BlackBerry UEM según la pertenencia del usuario al grupo universal o global de directorios de la empresa. Las cuentas de usuario se agregan a BlackBerry UEM durante el proceso de sincronización.

También puede optar por enviar automáticamente a los usuarios integrados un mensaje de correo y contraseñas de activación o claves de acceso para las aplicaciones de BlackBerry Dynamics.

Extracción

Si activa la integración, también puede elegir la configuración de la extracción. Cuando se desactiva un usuario en Microsoft Active Directory o se elimina de los grupos de directorios de la empresa en los grupos de directorios de integración, BlackBerry UEM puede extraer automáticamente al usuario de cualquiera de las formas siguientes:

- Eliminar los datos del trabajo o todos los datos de los dispositivos de usuarios
- Eliminar la cuenta de usuario de BlackBerry UEM

Puede utilizar la protección de la extracción para retrasar la eliminación de los datos de dispositivos o las cuentas de usuario para evitar las eliminaciones inesperadas debidas a la latencia de replicación de directorios. De forma predeterminada, la protección de la extracción retrasa las acciones de extracción durante dos horas después del siguiente ciclo de sincronización.

Nota: Los ajustes de extracción también se aplican a los usuarios del directorio en BlackBerry UEM. Se recomienda que haga clic en el icono de vista previa para generar el informe de sincronización de directorios y verificar los cambios.

Sincronización

Tras activar la extracción, durante la siguiente sincronización, las reglas de extracción se aplican a todos los usuarios que haya agregado manualmente en la consola de gestión antes de activar la extracción y que no sean miembros de grupos de integración vinculados a directorios.

Tras activar la integración, puede agregar manualmente usuarios a BlackBerry UEM aunque ya estén en un grupo vinculado a directorios. Si se activa la extracción, se aplicarán reglas de extracción a los dispositivos de los usuarios que agregue manualmente a BlackBerry UEM cuando se produzca la siguiente sincronización, en caso de que no sean miembros de un grupo de sincronización de integración en el momento de la sincronización.

Activación y configuración de la integración y la extracción

Puede integrar usuarios de forma automática que sean miembros de grupos universales y globales. La integración no es compatible con los grupos de dominios locales.

Antes de empezar:

- Verifique que una sincronización del directorio de la empresa no esté en curso. No puede guardar los cambios que realice en la conexión del directorio de la empresa hasta que se haya completado la sincronización.
- Para integrar miembros de grupos globales, debe activar la compatibilidad con grupos globales en la configuración de su conexión a Microsoft Active Directory.

1. En la barra de menús, haga clic en **Configuración > Integración externa > Directorio de la empresa**.
2. Haga clic en el nombre del directorio de la empresa que desea editar.
3. En la pestaña **Sincronizar configuración**, seleccione la casilla de verificación **Permitir los grupos vinculados a directorios**.
4. Seleccione la casilla de verificación **Permitir integración**.
5. Realice las acciones siguientes para cada grupo que desee configurar para la integración con la opción de activación del dispositivo:
   a) Haga clic en +.
   b) Escriba un nombre del grupo de directorios de la empresa. Haga clic en 🔍.
   c) Seleccione el grupo. Haga clic en **Agregar**.
   d) Opcionalmente, seleccione **Vincular grupos anidados**.
   e) En la sección **Activación del dispositivo**, seleccione si desea que los usuarios integrados reciban una contraseña de activación generada automáticamente o que no haya contraseña de activación. Si selecciona la opción de contraseña generada automáticamente, configure el periodo de activación y seleccione una plantilla de correo de activación.
6. Para integrar usuarios con BlackBerry Dynamics, seleccione la casilla de verificación **Integrar usuarios con las aplicaciones de BlackBerry Dynamics solamente**.
7. Realice las siguientes acciones para cada grupo que desee integrar con la activación para aplicaciones de BlackBerry Dynamics solamente:
   a) Haga clic en +.
   b) Escriba un nombre del grupo de directorios de la empresa. Haga clic en 🔍.
   c) Seleccione el grupo. Haga clic en **Agregar**.
   d) Opcionalmente, seleccione **Vincular grupos anidados**.
   e) Seleccione el número de claves de acceso que se generarán por usuario agregado, la caducidad de la clave de acceso y la plantilla de correo electrónico.
8. Para eliminar los datos del dispositivo cuando se extrae un usuario, seleccione la casilla de verificación **Eliminar los datos del dispositivo cuando el usuario se haya eliminado de todos los grupos de directorios de integración**. Seleccione una de las siguientes opciones:
   - Eliminar solo los datos de trabajo
   - Eliminar todos los datos del dispositivo
   - Eliminar todos los datos de los dispositivos de empresa/eliminar únicamente los datos de trabajo de los dispositivos personales
9. Para eliminar una cuenta de usuario de BlackBerry UEM cuando un usuario se elimina de todos los grupos de integración, seleccione **Eliminar usuario cuando el usuario se haya eliminado de todos los grupos de directorio de integración**. La primera vez que se produce un ciclo de sincronización después de que una cuenta de usuario se elimine de todos los grupos de directorios de integración, la cuenta de usuario se elimina de BlackBerry UEM.

10. Para evitar que las cuentas de usuario o los datos de dispositivo se eliminen de BlackBerry UEM inesperadamente, seleccione **Protección de la extracción**.

    La protección de la extracción implica que los usuarios no se borrarán de BlackBerry UEM hasta dos horas después del siguiente ciclo de sincronización.

11. Para forzar la sincronización de los grupos de directorios de la empresa, seleccione la casilla de verificación **Forzar sincronización**.

    Si se selecciona, cuando un grupo se elimina del directorio de la empresa, los vínculos a ese grupo se eliminan de los grupos de directorios de integración y los grupos vinculados a directorios. Si no se selecciona, en caso de no encontrar un grupo de directorios de la empresa, el proceso de sincronización se cancela.

12. En el campo **Límite de sincronización**, escriba el número máximo de cambios que desea permitir para cada proceso de sincronización. La configuración predeterminada es cinco.

    Si el número de cambios que deben sincronizarse supera el límite de sincronización, puede impedir que se ejecute el proceso de sincronización. Los cambios se calculan sumando lo siguiente: los usuarios que se agregarán a los grupos, los usuarios que se eliminarán de los grupos, los usuarios que se van a integrar y los usuarios que se van a extraer.

13. En el campo **Nivel máximo de anidamiento de grupos de directorio**, escriba el número de niveles anidados para grupos de directorios de la empresa.
14. Haga clic en **Guardar**.

Sincronización de una conexión de directorio de empresa

Antes de empezar: Vista previa del informe de sincronización

1. En la barra de menús, haga clic en **Configuración > Integración externa > Directorio de la empresa**.
2. En la columna **Sincronizar**, haga clic en .

Después de terminar: Visualización de un informe de sincronización

Vista previa del informe de sincronización

La vista previa de un informe de sincronización le permite verificar que las actualizaciones planificadas son las esperadas antes de que se realice la sincronización.

1. En la barra de menús, haga clic en **Configuración > Integración externa > Directorio de la empresa**.
2. En la columna **Vista previa**, haga clic en .
3. Haga clic en **Previsualizar ahora**.
4. Cuando termine de procesar el informe, haga clic en la fecha en la columna **Último informe**.
5. Para ver los informes de sincronización que se generaron previamente, haga clic en el menú desplegable.

Visualización de un informe de sincronización

1. En la barra de menús, haga clic en **Configuración > Integración externa > Directorio de la empresa**.
2. En la columna **Último informe**, haga clic en la fecha.
3. Para ver los informes de sincronización que se generaron previamente, haga clic en el menú desplegable.
4. Para exportar un archivo .csv del informe, haga clic en .

Agregar un programa de sincronización

Puede agregar un programa de sincronización para sincronizar BlackBerry UEM automáticamente con el directorio de la empresa. Hay tres tipos de programas de sincronización:

- Intervalo: Especifica el tiempo entre cada sincronización, el marco de tiempo y los días en que se producirá.
- Una vez al día: Permite especificar la hora del día en que empieza la sincronización y los días en los que se producirá.
- Sin periodicidad: Permite especificar la hora y el día de una sincronización única.

En la pantalla Directorio de la empresa, puede sincronizar manualmente BlackBerry UEM con el directorio de la empresa en cualquier momento.

1. En la barra de menús, haga clic en **Configuración > Integración externa > Directorio de la empresa**.
2. Haga clic en el nombre del directorio de la empresa que desea editar.
3. En la pestaña **Programación de sincronización**, haga clic en +.
4. Para reducir la cantidad de información que se sincroniza, en la lista desplegable **Tipo de sincronización**, elija una de las siguientes opciones:
   - **Todos los grupos y usuarios**: Esta es la configuración predeterminada. Si selecciona esta opción, los usuarios se integrarán, extraerán y vincularán a los grupos vinculados del directorio pertinente durante la sincronización. Se sincronizarán los usuarios que no se integren ni extraigan, pero que cambien de grupos vinculados a directorios, y aquellos con cambios en sus atributos.
   - **Incorporación de grupos**: Si selecciona esta opción, los usuarios se incorporarán, eliminará y vincularán a los grupos vinculados del directorio pertinente durante la sincronización y se sincronizarán aquellos usuarios con cambios en sus atributos. Los usuarios que no se integren ni se extraigan, pero que cambien de grupos vinculados a directorios no se vincularán.
   - **Grupos vinculados a directorios**: Si elige esta opción, los usuarios no podrán incorporarse ni eliminarse durante la sincronización. Los usuarios con cambios en sus grupos vinculados a directorios se vincularán adecuadamente. Los usuarios con cambios en sus atributos se sincronizarán.
   - **Atributos de usuario**: Si elige esta opción, los usuarios no podrán incorporarse ni eliminarse durante la sincronización. Los usuarios con cambios en sus grupos vinculados a directorios no se sincronizarán. Los usuarios con cambios en sus atributos se sincronizarán.
5. En la lista desplegable **Repetición**, seleccione una de las opciones siguientes:

Opción	Pasos
Intervalo	**a.** En el campo **Intervalo**, escriba el tiempo, en minutos, entre las sincronizaciones. **b.** Especifique el intervalo de tiempo de sincronización. **c.** Seleccione los días de la semana en que desea que las sincronizaciones se lleven a cabo.
Una vez al día	**a.** Especifique cuándo desea que se inicie la sincronización. **b.** Seleccione los días de la semana en que desea que las sincronizaciones se lleven a cabo.
Sin periodicidad	**a.** Especifique cuándo desea que se inicie la sincronización. **b.** Seleccione el día en que desea que la sincronización se lleve a cabo.

6. Haga clic en **Agregar**.

Eliminación de una conexión a un directorio de la empresa

Si elimina una conexión a un directorio de la empresa, todos los usuarios que se agregaron a BlackBerry UEM desde ese directorio de la empresa se convertirán en usuarios locales. Una vez que los usuarios se convierten en usuarios locales, no se pueden volver a convertir en usuarios vinculados a directorios, ni siquiera si posteriormente vuelve a agregar la conexión al directorio de la empresa. Los usuarios seguirán funcionando como usuarios locales, pero UEM no podrá sincronizar las actualizaciones del directorio de la empresa, como los cambios de nombre, la dirección de correo electrónico y otros atributos.

1. En la barra de menús, haga clic en **Configuración > Integración externa > Directorio de la empresa**.
2. Haga clic en la **X** que se encuentra junto a la entrada del directorio de la empresa que desea eliminar.
3. Haga clic en **Eliminar**.

Conexión a un servidor SMTP para enviar notificaciones de correo

Para permitir a BlackBerry UEM el envío de notificaciones por correo, debe conectar BlackBerry UEM a un servidor SMTP.

BlackBerry UEM utiliza las notificaciones de correo para enviar instrucciones de activación a los usuarios. También se puede configurar BlackBerry UEM para que envíe contraseñas para las advertencias de BlackBerry UEM Self-Service y de cumplimiento de los dispositivos, y puede enviar mensajes de correo a las personas.

Si no conecta BlackBerry UEM a un servidor SMTP, BlackBerry UEM no puede enviar contraseñas, mensajes de activación o mensajes de correo. Continúa pudiendo configurar BlackBerry UEM para que envíe advertencias de cumplimiento directamente a los dispositivos.

Para obtener más información acerca de los mensajes de activación, las advertencias de cumplimiento de los dispositivos y el envío de mensajes de correo individuales, consulte el contenido referente a Administración.

Conexión a un servidor SMTP para enviar notificaciones de correo

1. En la barra de menús, haga clic en **Configuración > Integración externa > Servidor SMTP**.
2. Haga clic en ✎.
3. En el campo **Nombre para mostrar del remitente**, escriba un nombre para utilizarlo en las notificaciones de correo de BlackBerry UEM. Por ejemplo, `donotreply` o `BUEM Admin`.
4. En el campo **Dirección del remitente**, escriba la dirección de correo que desea que BlackBerry UEM utilice para enviar notificaciones por correo.
5. En el campo **Servidor SMTP**, escriba el FQDN del servidor SMTP. Por ejemplo, `correo.ejemplo.com`.
6. En el campo **Puerto de servidor SMTP**, escriba el número de puerto de servidor SMTP. El número de puerto predeterminado es el 25.
7. En el menú desplegable **Tipo de cifrado compatible**, seleccione el tipo de cifrado que desea aplicar a los mensajes de correo.
8. Si el servidor SMTP requiere autenticación, en el campo **Nombre de usuario**, escriba el nombre de inicio de sesión del servidor SMTP. En el campo **Contraseña**, escriba la contraseña del servidor SMTP.
9. Si es necesario, importe un certificado de CA SMTP:
   a) Copie el archivo de certificado SSL para el servidor SMTP de la empresa en el equipo que está utilizando.
   b) Haga clic en **Examinar**.
   c) Navegue hasta el archivo de certificado SSL y haga clic en **Cargar**.
10. Haga clic en **Guardar**.

Después de terminar: Haga clic en **Probar conexión** si desea probar la conexión con el servidor SMTP y enviar un mensaje de correo de prueba. BlackBerry UEM envía el mensaje a la dirección de correo especificada en el campo **Dirección del remitente**.

Configuración de replicación de bases de datos

Puede utilizar la replicación de bases de datos para proporcionar una alta disponibilidad a la base de datos de BlackBerry UEM. La replicación de bases de datos es una función de Microsoft SQL Server que permite mantener el servicio de base de datos y la integridad de los datos si ocurren problemas con la base de datos de BlackBerry UEM. Para obtener más información sobre la creación de reflejo de la base de datos, consulte el contenido de Planificación.

Nota: Microsoft tiene pensado dejar de usar la replicación de bases de datos en versiones futuras de Microsoft SQL Server y recomienda el uso de la función AlwaysOn para la alta disponibilidad de bases de datos. El uso de AlwaysOn requiere pasos de configuración antes de instalar BlackBerry UEM. Para obtener más información acerca del uso de AlwaysOn, consulte el contenido de Planificación.

Pasos para configurar la replicación de la base de datos

Para configurar la replicación de la base de datos, realice las siguientes acciones:

Paso	Acción
1	Revise los requisitos en el contenido de Planificación y compruebe que el dominio de BlackBerry UEM cumpla con los requisitos previos.
2	Cree la base de datos replicada, inicie una sesión de replicación y configure un servidor testigo.
3	Configure cada instancia de BlackBerry UEM para que se conecte a la base de datos replicada.

Requisitos previos: Configuración de replicación de bases de datos

- Configure el servidor principal y el de réplicas para permitir el acceso desde equipos remotos.
- Configure el servidor principal y el de réplicas para que tengan los mismos permisos.
- Configure un servidor testigo que utilizará para controlar el servidor principal.
- Configure el agente de Microsoft SQL Server para utilizar una cuenta de usuario de dominio con los mismos permisos administrativos locales que la cuenta de Windows que ejecuta el servicio BlackBerry UEM.
- Compruebe que la cuenta de usuario de dominio tenga permisos tanto para el servidor principal como para el de réplicas.
- Compruebe que el servidor DNS se está ejecutando.
- En cada equipo que aloje una instancia de base de datos de BlackBerry UEM, en el SQL Server 2012 Native Client, desactive la opción Canalizaciones con nombre. Si elige no desactivar la opción Canalizaciones con nombre, visite https://support.blackberry.com/community y lea el artículo 34373.
- Para revisar requisitos previos adicionales para la versión de Microsoft SQL Server de la empresa, visite technet.microsoft.com/sqlserver y lea Creación de reflejo de la base de datos: SQL Server 2012 o Creación de reflejo de la base de datos: SQL Server 2014.
- Si la base de datos replicada utiliza la instancia predeterminada, los componentes de BlackBerry UEM pueden conectarse a la base de datos replicada únicamente mediante el puerto predeterminado 1433, no mediante un puerto estático personalizado. Esto se debe a una limitación de Microsoft SQL Server 2005 y versiones

posteriores. Para obtener más información acerca de este problema, consulte Controlador JDBC SQL 2005 y la creación de reflejo de la base de datos.

Creación y configuración de la base de datos replicada

Antes de empezar: Para mantener la integridad de la base de datos al crear y configurar la réplica, detenga los servicios de BlackBerry UEM en cada equipo que aloje una instancia de BlackBerry UEM.

1. En Microsoft SQL Server Management Studio, navegue hasta la base de datos principal.
2. Cambie la propiedad **Modelo de recuperación** a **COMPLETO**.
3. En el editor de consultas, ejecute la consulta **-- ALTER DATABASE** <*BUEM_db*> **SET TRUSTWORTHY ON**, en la que <*BUEM_db*> es el nombre de la base de datos principal.
4. Haga una copia de seguridad de la base de datos principal. Cambie la opción **Tipo de copia de seguridad** a **Completo**.
5. Copie los archivos de copia de seguridad en el servidor de réplicas.
6. En el servidor de réplicas, restaure la base de datos para crear la réplica. Al restaurar la base de datos, seleccione la opción **SIN RECUPERACIÓN**.
7. Verifique que el nombre de la base de datos replicada coincida con el nombre de la principal.
8. En el servidor principal, en Microsoft SQL Server Management Studio, haga clic con el botón derecho en la base de datos principal y seleccione la tarea **Replicar**. En la página **Replicación**, haga clic en **Configurar seguridad** para iniciar el Asistente para la configuración de seguridad de la creación de reflejo de bases de datos.
9. Inicie el proceso de replicación. Para obtener más información, consulte Configurar la creación de reflejo de la base de datos: SQL Server 2012 o Configurar la creación de reflejo de la base de datos: SQL Server 2014.
10. Para permitir la conmutación por error automática, agregue un testigo de la sesión de replicación. Para obtener más información, consulte Testigo de creación de reflejo de la base de datos: SQL Server 2012 o Testigo de creación de reflejo de la base de datos: SQL Server 2014.

Después de terminar:

- Para verificar que la conmutación por error funcione correctamente, conmute por error el servicio manualmente a la base de datos replicada y vuelva a la principal.
- Reinicie los servicios de BlackBerry UEM en cada equipo que aloje una instancia de BlackBerry UEM. No se detenga e inicie BlackBerry UEM: BlackBerry Work Connect Notification Service; este servicio se reinicia automáticamente al reiniciar el servicio BlackBerry UEM: BlackBerry Affinity Manager.
- Conexión de BlackBerry UEM con la base de datos replicada.

Conexión de BlackBerry UEM con la base de datos replicada

Debe repetir la tarea en cada equipo que aloje una instancia de BlackBerry UEM. Si el único componente de BlackBerry UEM de un equipo es BlackBerry Router, no tendrá que completar esta tarea en ese equipo.

Antes de empezar:

- Creación y configuración de la base de datos replicada.
- Verifique que se esté ejecutando el servidor de réplicas.
- Puede realizar esta tarea utilizando la herramienta de configuración de BlackBerry UEM o puede actualizar manualmente el archivo de propiedades de la base de datos siguiendo las siguientes instrucciones. Si desea utilizar la herramienta de configuración de BlackBerry UEM, visite support.blackberry.com/community y

consulte el artículo KB36443. En la sección "Actualización de las propiedades de la base de datos BlackBerry UEM siga las instrucciones para activar el reflejo de SQL y proporcionar el FQDN del servidor de réplicas.

1. En el equipo que aloja la instancia de BlackBerry UEM, vaya hasta *<unidad>*:\Archivos de programa\BlackBerry\UEM\common-settings.
2. En un editor de texto, abra **DB.properties**.
3. En la sección **configuración opcional para utilizar la conmutación por error**, después de **configuration.database.ng.failover.server=**, escriba el FQDN del servidor de réplicas (por ejemplo, `configuration.database.ng.failover.server=mirror_server.domain.net`).
4. Si es necesario, realice una de las siguientes acciones:
   - Si se especifica una instancia con nombre para la base de datos principal durante la instalación y la replicada utiliza la instancia predeterminada, elimine el valor después de **configuration.database.ng.failover.instance=**.
   - Si la base de datos principal utiliza una instancia predeterminada y la replicada utiliza una instancia con nombre, después de **configuration.database.ng.failover.instance=**, escriba la instancia con nombre.
5. Guarde y cierre **DB.properties**.

Después de terminar:

- Reinicie los servicios BlackBerry UEM. No se detenga e inicie BlackBerry UEM: BlackBerry Work Connect Notification Service; este servicio se reinicia automáticamente al reiniciar el servicio BlackBerry UEM: BlackBerry Affinity Manager.
- Repita la tarea en cada equipo que aloje una instancia de BlackBerry UEM.
- Compruebe que cada equipo que aloja una instancia de BlackBerry UEM pueda conectarse al servidor de réplicas mediante el nombre abreviado del servidor.

Configuración de una nueva base de datos replicada

Si crea y configura una nueva base de datos replicada después de que se produzca un cambio de función (es decir, los componentes de BlackBerry UEM conmutaron por error la base de datos replicada actual y, de este modo, se convirtió en la principal), repita Conexión de BlackBerry UEM con la base de datos replicada en cada equipo que aloje una instancia de BlackBerry UEM.

Conexión de BlackBerry UEM a Microsoft Azure

Microsoft Azure es el servicio informático en la nube de Microsoft para la implementación y la gestión de aplicaciones y servicios. Debe conectar BlackBerry UEM a Azure si desea usar BlackBerry UEM para implementar aplicaciones iOS y Android gestionadas por Microsoft Intune, si desea usar el acceso condicional de Azure Active Directory o si desea gestionar aplicaciones de Windows 10 en BlackBerry UEM.

BlackBerry UEM admite la configuración de un único inquilino Azure. Para conectar BlackBerry UEM a Azure, debe realice las acciones siguientes:

Paso	Acción
1	Crea una cuenta de Microsoft Azure.
2	Sincronización de Microsoft Active Directory con Microsoft Azure.
3	Creación de un extremo empresarial en Azure.
4	Configure BlackBerry UEM para que se sincronice con Microsoft Intune y Windows Store for Business.
5	(Opcional) Configure el acceso condicional de Azure Active Directory.

Crea una cuenta de Microsoft Azure

Para implementar aplicaciones protegidas por Microsoft Intune a dispositivos iOS y Android o administrar aplicaciones Windows 10 en BlackBerry UEM, debe tener una cuenta Microsoft Azure y autenticar BlackBerry UEM con Azure.

Complete esta tarea si su empresa no tiene una cuenta de Microsoft Azure.

Nota: Para asegurarse de que tiene las licencias y los permisos de cuenta correctos para Microsoft Intune, visite support.blackberry.com/community para leer el artículo 50341.

1. Vaya a https://azure.microsoft.com y haga clic en **Cuenta gratuita**; a continuación, siga las indicaciones para crear la cuenta.

   Se le solicitará que proporcione información de la tarjeta de crédito para crear la cuenta.
2. Regístrese en el portal de gestión Azure en https://portal.azure.com e inicie sesión con el nombre de usuario y contraseña que creó al registrarse.

Después de terminar: Sincronización de Microsoft Active Directory con Microsoft Azure.

Sincronización de Microsoft Active Directory con Microsoft Azure

Para permitir que los usuarios de Windows 10 puedan instalar aplicaciones en línea o enviar aplicaciones protegidas por Microsoft Intune a los dispositivos iOS y Android, deben existir usuarios en Microsoft Azure Active Directory. debe sincronizar los usuarios y grupos entre sus versiones locales de Active Directory y Azure Active Directory mediante Microsoft Azure Active Directory Connect. Para obtener más información, visite https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect.

1. Descarga Azure AD Connect del Centro de descarga de Microsoft.
2. Instalar el software de Azure AD Connect.
3. Configure Azure AD Connect para conectar su Active Directory local con Azure Active Directory.

Después de terminar: Creación de un extremo empresarial en Azure

Creación de un extremo empresarial en Azure

Para que BlackBerry UEM pueda acceder a Microsoft Azure, debe crear un extremo empresarial dentro de Azure. El extremo empresarial permite a BlackBerry UEM autenticarse en Microsoft Azure. Para obtener más información, consulte https://docs.microsoft.com/en-us/azure/active-directory/active-directory-app-registration.

Si va a conectar BlackBerry UEM tanto a Microsoft Intune como a la Windows Store para empresas, utilice una aplicación empresarial diferente para cada fin debido a las diferencias en los permisos y los posibles cambios futuros.

Nota:

Las implementaciones de nubes nacionales de Microsoft (o cualquier implementación que requiera una URL de inicio de sesión distinta de login.microsoftonline.com) requieren pasos adicionales para conectar UEM con Intune. Para obtener más información, visite support.blackberry.com/community y lea el artículo KB75773.

Antes de empezar:

-
- Asegúrese de tener una URL de respuesta. Para obtener más información sobre cómo obtener la URL de respuesta para las autenticaciones modernas, consulte Configurar BlackBerry UEM para su sincronización con Microsoft Intune.

1. Inicie sesión en el portal de Azure.
2. Vaya a **Microsoft Azure > Azure Active Directory > Registros de aplicaciones**.
3. Haga clic en **Nuevo registro**.
4. En el campo **Nombre**, escriba un nombre para la aplicación.
5. Seleccione los tipos de cuenta que usarán la aplicación o accederán a la API.
6. En la sección **URI de redireccionamiento**, en la lista desplegable, seleccione **Mobile Client/Desktop** e introduzca una URL válida. El formato de URL es https://<*FQDN_del_servidor_de_BlackBerry_UEM*>:<*puerto*>/admin/intuneauth
7. Haga clic en **Registrar**.
8. Copie el **ID de aplicación** de su aplicación y péguelo en un archivo de texto.

   Este es el **ID de cliente** que se requiere en BlackBerry UEM.
9. Si va a crear la aplicación para utilizar Microsoft Intune, haga clic en **Permisos de API** en la sección **Administrar**. Realice los siguientes pasos:
   a) Haga clic en **Agregar un permiso**.
   b) Haga clic en **Microsoft Graph**.

c) Seleccione **Permisos delegados**.
d) Desplácese hacia abajo por la lista de permisos y en **Permisos delegados** establezca los siguientes permisos para Microsoft Intune:
   - Lea y escriba aplicaciones de Microsoft Intune (**DeviceManagementApps > DeviceManagementApps.ReadWrite.All**)
   - Lea todos los grupos (**Group > Group.Read.All**)
   - Lea el perfil básico de todos los usuarios (**User > User.ReadBasic.All**)
e) Haga clic en **Agregar permisos**.
f) En **Conceder consentimiento**, haga clic en **Conceder consentimiento de administrador**.

   Nota: Debe ser un administrador global para conceder los permisos.
g) Cuando se le solicite, haga clic en **Sí** para conceder permisos para todas las cuentas en el directorio actual.

Puede utilizar los permisos predeterminados si va a crear la aplicación para que se conecte a Windows Store for Business.

10. Haga clic en **Certificados y secretos** en la sección **Administrar**. Realice las acciones siguientes:
a) En **Secretos de cliente**, haga clic en **Nuevo secreto de cliente**.
b) Escriba una descripción para el secreto de cliente.
c) Seleccione una duración para el secreto de cliente.
d) Haga clic en **Agregar**.
e) Copie el valor del nuevo secreto de cliente.

   Esta es la **Clave de cliente** que se requiere en BlackBerry UEM.

   Advertencia: Si no copia el valor de su clave en este momento, tendrá que crear una nueva clave porque el valor no se mostrará después de salir de esta pantalla.

Después de terminar: Configurar BlackBerry UEM para su sincronización con Microsoft Intune o Configurar BlackBerry UEM para su sincronización con la Tienda Windows para empresas.

Configuración del acceso condicional de Azure Active Directory

Si ha configurado el acceso condicional de Azure AD para su empresa, puede configurar un inquilino BlackBerry UEM como socio de cumplimiento para que los dispositivos con iOS y Android administrados por UEM puedan conectarse a sus aplicaciones basadas en la nube, tales como Office 365. Solo puede configurar un inquilino de UEM por cada inquilino Azure.

Nota: El soporte de acceso condicional de Azure AD está limitado en este momento en las siguientes situaciones:

- BlackBerry UEM Client No admite políticas de acceso condicional de Azure AD con la opción "Todas las aplicaciones en la nube" seleccionada en "Aplicaciones en la nube" o "Acciones". En su lugar, debe seleccionar las aplicaciones específicas que desea incluir en la política. Para obtener más información, visite support.blackberry.com/community y lea el artículo 90010.
- BlackBerry Work no admite la función de cumplimiento de acceso condicional de Azure AD. Para obtener más información, visite support.blackberry.com/community y lea el artículo 89668.

Para utilizar esta función, el entorno de la empresa debe cumplir con los requisitos siguientes:

- Los usuarios deben existir en Azure AD,
- Si está sincronizando su Active Directory local a Azure AD, la UPN de Active Directory local de los usuarios debe coincidir con su UPN de Azure AD. Si estos valores no coinciden en su entorno, visite support.blackberry.com/community para leer el artículo 88208.

- Los usuarios deben agregarse UEM a aunque se sincronice con Active Directory.
- A los usuarios se les debe asignar un perfil de BlackBerry Dynamics que tenga seleccionado "Activar UEM Client para que pueda inscribirse en BlackBerry Dynamics".
- Los usuarios deben tener la aplicación Authenticator Microsoft instalada y BlackBerry UEM Client instalada.

Si configura el acceso condicional de Azure AD, UEM notifica a Azure AD cuando un dispositivo esté fuera de los requisitos de cumplimiento y las condiciones se aplican en las siguientes circunstancias:

- Si la configuración de "Acción de cumplimiento para dispositivo" está establecida en una opción distinta de "Supervisar y registrar", UEM notifica a Azure AD después de que todas las solicitudes de usuario hayan caducado.
- Si la configuración de la "Acción de cumplimiento para aplicaciones BlackBerry Dynamics" está establecida en una opción distinta de "Supervisar y registrar", UEM notifica a Azure AD tan pronto como se detecte la infracción de cumplimiento.

Para obtener más información sobre los perfiles de cumplimiento, consulte el contenido de Administración de UEM.

Para obtener más información sobre el acceso condicional a Azure AD, consulte la documentación de Microsoft.

Configuración de acceso condicional de Azure Active Directory.

Antes de empezar: Debe utilizar las licencias E5 de Microsoft 365. Para obtener más información, visite support.blackberry.com y lea los artículos KB91041 y KB50341. Para obtener más información sobre las licencias, consulte los detalles de Microsoft.

1. En el centro de administración de Microsoft Endpoint Manager, en **Administración de inquilinos > Conectores y tokens > Administración de cumplimiento para socios** añada **BlackBerry UEM** como socio de cumplimiento para dispositivos con iOS y Android y para asignarlo a usuarios y grupos.

   Si es compatible con dispositivos con iOS y Android, debe agregar BlackBerry UEM como socio de cumplimiento para cada plataforma. Para obtener más información, consulte la documentación de Microsoft.
2. En la consola de administración de BlackBerry UEM, haga clic en **Configuración > Integración externa > Acceso condicional de Azure Active Directory**.
3. Seleccione **Activar acceso condicional**.
4. En la lista desplegable **Azure Cloud**, seleccione **Global**.
5. Introduzca su **ID de inquilino de Azure**.

   Puede introducir el nombre del grupo de usuarios, que está en formato FQDN, o el ID único del grupo de usuarios, que está en formato GUID.
6. Haga clic en **Guardar**.
7. Seleccione la cuenta de administrador que desea utilizar para iniciar sesión en su Azure inquilino.

   La cuenta de administrador debe ser capaz de otorgar permisos a la aplicación para acceder a los recursos de su empresa. como el administrador global, el administrador de aplicaciones en la nube o el administrador de aplicaciones.
8. Acepte la solicitud de permiso de Microsoft.
9. En la consola de administración de BlackBerry UEM, edite cada perfil de conectividad de BlackBerry Dynamics y lleve a cabo las siguientes acciones:
   a) En **Servidores de aplicaciones**, haga clic en **Agregar**.
   b) Seleccione **Función-Acceso condicional de Azure** en la lista de aplicaciones.
   c) Haga clic + para agregar un nuevo servidor de aplicaciones.
   d) Si está utilizando BlackBerry UEM en un entorno local, especifique la siguiente configuración del servidor:

Elemento	Descripción
Servidor	gdas-<SRP_ID>.<region_code>.bbsecure.com
Puerto	443
Ruta	Directo

Si tiene BlackBerry UEM Cloud y BEMS Cloud en su entorno y ha configurado notificaciones de correo electrónico o BEMS-Docs para crear un inquilino de BEMS, la URL, el número de puerto y la prioridad de BEMS Cloud se agregan automáticamente a la sección de carga del servidor de aplicaciones.

10. Asigne la aplicación **Función-Acceso condicional de Azure** a usuarios o grupos.
11. En el perfil de BlackBerry Dynamics, asegúrese de que esté seleccionada la configuración **Activar UEM Client para que pueda inscribirse en BlackBerry Dynamics**.

Después de terminar:

- La aplicación Microsoft Authenticator debe estar instalada en los dispositivos de los usuarios. Puede asignar la aplicación en UEM o indicar a los usuarios que la instalen desde su tienda de aplicaciones.
- Después de configurar el acceso condicional de Active Directory, se solicita a los usuarios que activen los dispositivos que se registren con acceso condicional de Active Directory durante la activación. Se solicita a los usuarios con dispositivos activados que se registren con acceso condicional de Active Directory la siguiente vez que abran UEM Client.

Quitar dispositivos del acceso condicional de Azure Active Directory

Cuando desactiva un dispositivo de BlackBerry UEM, el dispositivo permanece registrado para el acceso condicional de Azure AD. Azure reconoce que el dispositivo ya no se administra, lo que, según su configuración de acceso condicional, puede colocar el dispositivo fuera de los requisitos de cumplimiento.

Los usuarios pueden eliminar sus dispositivos de Azure mediante la eliminación de su cuenta de Azure AD de la configuración de la cuenta en la aplicación Microsoft Authenticator o puede eliminar el dispositivo de Azure.

1. En el portal Azure, en Azure AD, seleccione el usuario para el que desea eliminar el dispositivo.
2. Vea la página **Dispositivos** del usuario.
3. Seleccione el dispositivo y haga clic en **Aceptar**.

Permiso de acceso a BlackBerry Web Services mediante BlackBerry Infrastructure

Si su empresa utiliza un cliente de servicios Web que se encuentra fuera del firewall de la empresa y el cliente requiere acceso a las API de BlackBerry Web Services (REST o SOAP heredado), el cliente puede conectarse a las API de forma segura a través de BlackBerry Infrastructure. Para obtener más información acerca del permiso de acceso a las aplicaciones de cliente, los desarrolladores pueden consultar la sección Primeros pasos de la referencia de la API REST de BlackBerry Web Services.

Los clientes de servicios Web solo pueden usar BlackBerry Infrastructure para acceder a las API de BlackBerry Web Services si activa este acceso en la consolas de gestión. De forma predeterminada, este acceso no está activado.

1. En la barra de menús, haga clic en **Configuración > Configuración general > Acceso a BlackBerry Web Services**.
2. Haga clic en **Activar**.
3. Haga clic en **Guardar**.

Adquisición de certificado APN para gestionar los dispositivos iOS y macOS

APN es el servicio de Apple Push Notification. Debe obtener y registrar un certificado APN si desea utilizar BlackBerry UEM para gestionar dispositivos iOS o macOS. Si configuró más de un dominio de BlackBerry UEM, cada dominio requiere un certificado APN.

Puede obtener y registrar el certificado APN a través del primer asistente de inicio de sesión o de la sección de integración externa de la consola de gestión.

Nota: El certificado APN es válido durante un año. La consola de gestión muestra la fecha de caducidad. Deberá renovar el certificado APN antes de la fecha de caducidad, a través del mismo ID de Apple que utilizó para obtener el certificado. Puede anotar el ID de Apple en la consola de gestión. También puede crear una notificación de eventos por correo electrónico para que le recuerde que debe renovar el certificado 30 días antes de que caduque. Si el certificado caduca, los dispositivos no reciben datos de BlackBerry UEM. Si registra un nuevo certificado APN, los usuarios de dispositivos deberán reactivar los dispositivos para recibir datos.

Para obtener más información, visite https://developer.apple.com y lea *Problemas con el envío de notificaciones de inserción* en el artículo TN2265.

Es una práctica recomendada, acceder a la consola de gestión y al portal de certificados de inserción de Apple mediante el navegador Google Chrome o el Safari. Estos navegadores proporcionan una compatibilidad óptima para solicitar y registrar un certificado APN.

Para obtener y registrar un certificado APN, realice las siguientes acciones:

Paso	Acción
1	Obtener una CSR firmada de BlackBerry.
2	Usar la CSR firmada para solicitar un certificado APN de Apple.
3	Registro del certificado APN.

Obtener una CSR firmada de BlackBerry

Deberá obtener una CSR firmada de BlackBerry antes de que pueda obtener un certificado APN.

1. En la barra de menús, haga clic en **Configuración > Integración externa > Apple Push Notification**.
2. Si todavía no tiene un certificado APN, en la sección **Paso 1 de 3: Descargar el certificado CSR firmado de BlackBerry**, haga clic en **Descargar certificado**.

   Si desea renovar el certificado APN actual, haga clic en **Renovar certificado** en su lugar.
3. Haga clic en **Guardar** para guardar el archivo CSR firmado (.scsr) en el equipo.

Después de terminar: Solicitud de un certificado APN de Apple.

Solicitud de un certificado APN de Apple

Antes de empezar: Obtener una CSR firmada de BlackBerry.

1. En la barra de menús, haga clic en **Configuración > Integración externa > Apple Push Notification**.
2. En la sección **Paso 2 de 3: Solicitar un certificado APN de Apple**, haga clic en **Portal de certificados de inserción de Apple**. Se le dirige al portal de certificados de inserción de Apple.
3. Inicie sesión en el portal de certificados Push de Apple utilizando un ID de Apple válido.
4. Siga las instrucciones para cargar la CSR firmada (.scsr).
5. Descargue y guarde el certificado APN (.pem) en el equipo.
6. (Opcional) Haga clic en para mostrar la ventana **Nota**.
7. En la ventana **Nota**, escriba el ID de Apple que utilizó para solicitar el certificado APN.
   Debe utilizar el mismo ID de Apple para renovar el certificado.
8. Haga clic en cualquier sitio fuera de la ventana **Nota** para cerrarla.

Después de terminar: Registro del certificado APN.

Registro del certificado APN

Antes de empezar: Solicitud de un certificado APN de Apple.

1. En la barra de menús, haga clic en **Configuración > Integración externa > Apple Push Notification**.
2. En la sección **Paso 3 de 3: Registrar el certificado APN**, haga clic en **Examinar**. Vaya al certificado APN (.pem) y selecciónelo.
3. Haga clic en **Enviar**.

Después de terminar: Para probar la conexión entre BlackBerry UEM y el servidor de APN, haga clic en **Probar certificado APN**.

Renovación del certificado APN

El certificado APN es válido durante un año. Debe renovar el certificado APN cada año antes de que caduque. El certificado debe renovarse utilizando el mismo ID de Apple que utilizó para obtener el certificado APN original.

Puede crear una notificación de eventos por correo electrónico para que le recuerde que debe renovar el certificado 30 días antes de que caduque.

Antes de empezar: Obtener una CSR firmada de BlackBerry.

1. En la barra de menús, haga clic en **Configuración > Integración externa > Apple Push Notification**.
2. Haga clic en **Renovar certificado**.
3. En la sección **Paso 1 de 3: Descargar el certificado CSR firmado de BlackBerry**, haga clic en **Descargar certificado**.
4. Haga clic en **Guardar** para guardar el archivo CSR firmado (.scsr) en el equipo.
5. En la sección **Paso 2 de 3: Solicitar un certificado APN de Apple**, haga clic en **Portal de certificados de inserción de Apple**. Se le dirige al portal de certificados de inserción de Apple.
6. Inicie sesión en el portal de certificados de inserción de Apple a través del mismo ID de Apple que utilizó para obtener el certificado APN original.
7. Siga las instrucciones para renovar el certificado APN (.pem). Tendrá que cargar la nueva CSR firmada.

8. Descargue y guarde el certificado APN renovado en el equipo.
9. En la sección **Paso 3 de 3: Registrar el certificado APN**, haga clic en **Examinar**. Vaya al certificado APN renovado y selecciónelo.
10. Haga clic en **Enviar**.

Después de terminar: Para probar la conexión entre BlackBerry UEM y el servidor de APN, haga clic en **Probar certificado APN**.

Solución de problemas de APN

Esta sección le ayuda a solucionar problemas de APN.

El certificado APN no coincide con la CSR. Proporcione el archivo APN (.pem) correcto o envíe una nueva CSR.

Descripción

Puede recibir un mensaje de error al intentar registrar el certificado APN si no cargó el archivo CSR firmado más reciente desde BlackBerry al portal de certificados de inserción de Apple.

Solución posible

Si descargó varios archivos CSR de BlackBerry, solo el último archivo descargado es válido. Si sabe qué CSR es la más reciente, vuelva al portal de certificados de inserción de Apple y cárguela. Si no está seguro de cuál es la CSR más reciente, obtenga una nueva de BlackBerry, a continuación, vuelva al portal de certificados de inserción de Apple y cárguela.

Se muestra el mensaje "El sistema ha detectado un error" cuando intento obtener una CSR firmada

Descripción

Cuando intenta obtener una CSR firmada, se muestra el siguiente error: "El sistema ha detectado un error". Intente nuevamente”.

Solución posible

Visite support.blackberry.com y lea el artículo 37266.

No puedo activar dispositivos con iOS o macOS

Causa posible

Si no puede activar dispositivos iOS o macOS, el certificado APN podría no estar correctamente registrado.

Solución posible

Realice una o más de las acciones siguientes:

- En la consola de administración, en la barra de menús, haga clic en **Configuración > Integración externa > Apple Push Notification**. Compruebe que el estado del certificado APN es "Instalado". Si el estado no es correcto, intente registrar de nuevo el certificado APN.
- Haga clic en **Probar certificado APN** para probar la conexión entre BlackBerry UEM y el servidor APN.
- Si es necesario, obtenga una nueva CSR firmada de BlackBerry y un nuevo certificado APN.

Configuración de BlackBerry UEM para DEP

Debe configurar BlackBerry UEM para que utilice el programa de inscripción de dispositivos de Apple antes de poder sincronizar BlackBerry UEM con DEP. Después de configurar BlackBerry UEM, puede utilizar la consola de gestión de BlackBerry UEM para administrar la activación de los dispositivos iOS que haya adquirido la empresa para DEP.

Puede utilizar una cuenta de Apple Business Manager para 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.

Al configurar BlackBerry UEM para el programa de inscripción de dispositivos de Apple, deberá realizar las siguientes acciones:

Paso	Acción
1	Creación de una cuenta de DEP.
2	Descarga de una clave pública.
3	Generación de un identificador del servidor.
4	Registro del identificador del servidor con BlackBerry UEM.
5	Adición de la configuración de la primera inscripción.

Creación de una cuenta de DEP

1. En la barra de menús, haga clic en **Configuración > Integración externa > Programa de inscripción de dispositivos de Apple**.
2. Haga clic en +.
3. En el campo **Nombre**, escriba un nombre para la cuenta.
4. En el paso **1 de 4: Crear una cuenta de Apple DEP**, haga clic en **Crear una cuenta de Apple DEP**.
5. Complete los campos y siga las instrucciones para crear su cuenta.

Después de terminar: Descarga de una clave pública.

Descarga de una clave pública

Antes de empezar: Creación de una cuenta de DEP.

1. En la barra de menús, haga clic en **Configuración > Integración externa > Programa de inscripción de dispositivos de Apple**.

2. Haga clic en +.
3. En el paso **2 de 4: Descargar una clave pública**, haga clic en **Descargar clave pública**.
4. Haga clic en **Guardar**.

Después de terminar: Generación de un identificador del servidor.

Generación de un identificador del servidor

Antes de empezar: Descarga de una clave pública.

1. En la barra de menús, haga clic en **Configuración > Integración externa > Programa de inscripción de dispositivos de Apple**.
2. Haga clic en +.
3. En el paso **3 de 4: Generar el identificador del servidor desde la cuenta de Apple DEP**, haga clic en **Abra el portal de Apple DEP**.
4. Inicie sesión en la cuenta de DEP.
5. Siga las instrucciones para generar un identificador del servidor.

Después de terminar: Registro del identificador del servidor con BlackBerry UEM.

Registro del identificador del servidor con BlackBerry UEM

BlackBerry UEM utiliza un identificador del servidor para la autenticación cuando se comunica con el programa de inscripción de dispositivos de Apple.

Antes de empezar: Generación de un identificador del servidor.

1. En la barra de menús, haga clic en **Configuración > Integración externa > Programa de inscripción de dispositivos de Apple**.
2. Haga clic en +.
3. En el paso **4 de 4: Registrar el identificador del servidor con BlackBerry UEM**, haga clic en **Examinar**.
4. Seleccione el archivo de identificador del servidor **.p7m**.
5. Haga clic en **Abrir**.
6. Haga clic en **Siguiente**.

Después de terminar: Adición de la configuración de la primera inscripción.

Adición de la configuración de la primera inscripción

Antes de empezar: Registro del identificador del servidor con BlackBerry UEM antes de agregar la primera configuración de inscripción.

Después de registrar un identificador del servidor, BlackBerry UEM muestra automáticamente la ventana donde puede agregar la primera configuración de inscripción.

1. Escriba un nombre para la configuración.
2. Complete una de las tareas siguientes:

- Si desea que BlackBerry UEM asigne automáticamente la configuración de inscripción a los dispositivos al registrarlos en el Programa de inscripción de dispositivos de Apple, seleccione la casilla para marcar "Asignar automáticamente todos los nuevos dispositivos a esta configuración".
- Si desea utilizar la consola de BlackBerry UEM para asignar manualmente la configuración de inscripción a dispositivos específicos, no seleccione la casilla para marcar "Asignar automáticamente todos los nuevos dispositivos a esta configuración".

3. Opcionalmente, escriba el nombre de un departamento y un número de teléfono de soporte para que se muestren en los dispositivos durante la instalación.
4. En la sección **Configuración del dispositivo**, seleccione entre las siguientes casillas para marcar:
   - Permitir emparejamiento: si esta opción está seleccionada, los usuarios pueden emparejar el dispositivo con un ordenador
   - Obligatorio: si esta opción está seleccionada, los usuarios pueden activar los dispositivos mediante su nombre de usuario y contraseña del directorio de la empresa
   - Permitir la eliminación del perfil de MDM: si esta opción está seleccionada, los usuarios pueden desactivar los dispositivos.
   - 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.
5. 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, no puede 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
   - Tiempo en pantalla: si se selecciona, la opción para configurar el tiempo en pantalla se omitirá durante la inscripción en DEP
   - Actualización de software: si se selecciona, los usuarios no verán la pantalla de actualización de software obligatoria en el dispositivo
   - iMessage y Face Time: si se selecciona, los usuarios no verán las pantallas de iMessage y Face Time en el dispositivo
   - Tono para mostrar: si se selecciona, los usuarios no verán la pantalla de Tono para mostrar en el dispositivo
   - Privacidad: si se selecciona, los usuarios no verán la pantalla Privacidad en el dispositivo
   - Integración: si se selecciona, los usuarios no verán la pantalla informativa de integración en el dispositivo

- Migración de Watch: si se selecciona, los usuarios no verán la pantalla de migración de Watch en el dispositivo
- Configuración de SIM: si se selecciona, los usuarios no verán la pantalla para configurar un plan móvil en el dispositivo
- Migración de dispositivo a dispositivo: si se selecciona, los usuarios no verán la pantalla de migración de dispositivo a dispositivo en el dispositivo

6. Haga clic en **Guardar**.

   Si aparece el mensaje "Se ha detectado un error. No se ha podido descifrar el archivo del identificador de servidor.", visite support.blackberry.com/community y consulte el artículo 37282.
7. Si ha seleccionado "Asignar automáticamente los nuevos dispositivos a esta configuración", haga clic en **Sí**.

Después de terminar: Active los dispositivos iOS. Para obtener más información acerca de la activación de los dispositivos inscritos en DEP, consulte el contenido de Administración.

Actualización del identificador del servidor

El identificador del servidor es válido durante un año. Debe renovar el identificador cada año antes de que caduque. Para ver el estado del identificador, consulte la Fecha de caducidad en la ventana Programa de inscripción de dispositivos de Apple.

Antes de empezar: Si la clave pública ha cambiado, descargue una nueva clave pública.

1. En la barra de menús, haga clic en **Configuración > Integración externa > Programa de inscripción de dispositivos de Apple**.
2. Haga clic en el nombre de una cuenta de DEP.
3. En la sección **Fecha de caducidad**, haga clic en **Actualizar identificador del servidor**.
4. En el **Paso 1 de 2: Generar un identificador del servidor desde la cuenta de Apple DEP**, haga clic en **Abra el portal de Apple DEP**.
5. Inicie sesión en la cuenta de DEP.
6. Siga las instrucciones para generar un identificador del servidor.
7. En el paso **2 de 2: Registrar el identificador del servidor con BlackBerry UEM**, haga clic en **Examinar**.
8. Seleccione el archivo de identificador del servidor **.p7m**.
9. Haga clic en **Abrir**.
10. Haga clic en **Guardar**.

Eliminar conexión de DEP

PRECAUCIÓN: Si se eliminan todas las conexiones de DEP, no podrá activar los nuevos dispositivos iOS en el programa de inscripción de dispositivos de Apple. Si se ha asignado configuraciones de inscripción a los dispositivos y no se han aplicado, BlackBerry UEM elimina las configuraciones de inscripción asignadas a los dispositivos. La eliminación de la conexión no afecta a los dispositivos que están activados en BlackBerry UEM.

Si la empresa ya no implementa los dispositivos iOS que utilizan DEP, puede eliminar las conexiones de BlackBerry UEM con DEP.

1. En la barra de menús, haga clic en **Configuración > Integración externa > Programa de inscripción de dispositivos de Apple**.
2. Haga clic en el nombre de una cuenta de DEP.

3. Haga clic en **Eliminar conexión de DEP**.
4. Haga clic en **Eliminar**.
5. Haga clic en **Aceptar**.

Configuración de BlackBerry UEM para que admita dispositivos Android Enterprise

Los dispositivos Android Enterprise proporcionan un nivel de seguridad adicional para las empresas que quieren gestionar dispositivos Android. Para obtener más información acerca de los dispositivos Android Enterprise, visite https://support.google.com/work/android/.

Para obtener instrucciones detalladas acerca de la configuración de BlackBerry UEM para que admita dispositivos Android Enterprise, visite support.blackberry.com/community y lea el artículo 37748.

Hay dos maneras de configurar BlackBerry UEM para que sea compatible con dispositivos Android Enterprise:

1. Conectar BlackBerry UEM a un dominio de Google Cloud o G Suite.

   Nota: Puede conectar únicamente un dominio de BlackBerry UEM a un dominio de Google.
2. Permita que BlackBerry UEM administre dispositivos Android Enterprise que hayan gestionado cuentas de Google Play. No necesita tener un dominio de Google para usar esta opción. Para obtener más información, consulte https://support.google.com/googleplay/work/.

La tabla siguiente resume las diferentes opciones para la configuración de dispositivos Android Enterprise:

Método para configurar BlackBerry UEM para que sea compatible con dispositivos Android Enterprise	Cuándo se debe elegir este método	Tipo de cuenta de usuario	Servicios de Google compatibles
Conecte BlackBerry UEM al dominio de G Suite	Tiene un dominio de G Suite en su empresa	Cuentas de G Suite (para empresas)	Compatible con todos los servicios de G Suite, como Gmail, Google Calendar y Drive. Compatible con la gestión de aplicaciones a través de Google Play.
Conecte BlackBerry UEM al dominio de Google Cloud	Tiene un dominio de Google Cloud en su empresa	Cuentas de Google Cloud, también conocidas como cuentas de Google gestionadas (para empresas)	Similar a G Suite pero sin acceso a productos de pago como Gmail, Google Calendar y Drive. Compatible con la gestión de aplicaciones a través de Google Play.

Método para configurar BlackBerry UEM para que sea compatible con dispositivos Android Enterprise	Cuándo se debe elegir este método	Tipo de cuenta de usuario	Servicios de Google compatibles
Permita que BlackBerry UEM administre dispositivos Android Enterprise como cuentas administradas de Google Play	No dispone de un dominio de Google en su empresa o Dispone de un dominio de Google que ya está conectado a un dominio de BlackBerry UEM y desea utilizar dispositivos Android Enterprise en un segundo dominio de BlackBerry UEM	Dispositivos Android Enterprise que hayan administrado cuentas de Google Play	Compatible con la gestión de aplicaciones a través de Google Play. Los servicios de Google no son compatibles.

Configuración de BlackBerry UEM para admitir dispositivos Android Enterprise

Puede conectar únicamente un dominio de BlackBerry UEM a su dominio de Google. Antes de conectar otro dominio de BlackBerry UEM, debe eliminar la conexión existente. Consulte Eliminación de la conexión con el dominio de Google.

1. En la barra de menús, haga clic en **Configuración > Integración externa > Android Enterprise**.
2. Lleve a cabo una de las tareas siguientes:

Tarea	Pasos
Use dispositivos Android Enterprise que hayan administrado cuentas de Google Play	**a.** Seleccione **Permitir que BlackBerry UEM gestione cuentas de Google Play**. **b.** Haga clic en **Siguiente**. **c.** En la ventana **Bring Android to Work**, inicie sesión con una cuenta de Google. Puede utilizar cualquier cuenta de Google o de Gmail. La cuenta que utilice se convertirá en la cuenta de administrador para el servicio **Utilizar Android en el trabajo**. **d.** Haga clic en **Comenzar**. **e.** Escriba el nombre de su empresa Haga clic en **Confirmar**. **f.** Haga clic en **Completar registro**. Volverá a la consola de gestión de BlackBerry UEM.

Tarea	Pasos
Utilizar un dominio de Google	a. Seleccione **Conectar BlackBerry UEM a su dominio de Google existente**. b. Haga clic en **Siguiente**. c. Complete los campos para crear una cuenta de servicio y haga clic en **Siguiente**. Para obtener instrucciones detalladas, visite support.blackberry.com/community y lea el artículo 37748.

3. Seleccione cómo quiere que las configuraciones de la aplicación se envíen a un dispositivo. Cualquier información que haya añadido en la configuración de la aplicación podrá proporcionarse mediante BlackBerry Infrastructure o la infraestructura de Google. Lleve a cabo una de estas acciones:
   - Seleccione **Enviar configuración de la aplicación mediante UEM Client** para enviar las configuraciones de la aplicación a través de BlackBerry Infrastructure.
   - Seleccione **Enviar configuración de la aplicación mediante Google Play** para enviar los detalles de la configuración de la aplicación a través de la infraestructura de Google.
4. Cuando se le solicite, haga clic en **Aceptar** para aceptar el conjunto de permisos para todas o algunas de las siguientes aplicaciones:
   - Google Chrome
   - BlackBerry Connectivity
   - + Servicios de BlackBerry Hub
   - BlackBerry Hub
   - Calendario de BlackBerry
   - Contactos de BlackBerry
   - Notas de BlackBerry
   - Tareas de BlackBerry
5. Haga clic en **Finalizar**.

Después de terminar: Complete los pasos para activar dispositivos Android Enterprise. Para obtener más información acerca de la activación del dispositivo, consulte "Activación de dispositivos" en el contenido de Administración.

Eliminación de la conexión con el dominio de Google

Puede conectar únicamente un dominio de BlackBerry UEM al dominio de Google Cloud o de G Suite. Antes de conectar otro dominio de BlackBerry UEM, debe eliminar la conexión existente.

Elimine la conexión a su dominio de Google antes de completar cualquiera de las tareas siguientes:

- Eliminar un dominio de BlackBerry UEM
- Conectar otra instancia de BlackBerry UEM a su dominio de Google Cloud o G Suite

Si no elimina la conexión a su dominio de Google, es posible que no pueda conectar el dominio de Google Cloud o G Suite a la nueva instancia de BlackBerry UEM. Si elimina la conexión de BlackBerry UEM, todos los dispositivos que se activaron con un tipo de activación de Android Enterprise se desactivarán.

1. En la barra de menús, haga clic en **Configuración > Integración externa**.
2. Haga clic en **Conexión de dominio de Google**.
3. Haga clic en **Eliminar conexión**.
4. Haga clic en **Eliminar**.

Eliminación de la conexión de dominio de Google con su cuenta de Google

Si ha configurado BlackBerry UEM para admitir dispositivos Android Enterprise, puede eliminar la conexión en Google.

1. Con la cuenta de Google que utilizó para configurar dispositivos Android Enterprise, inicie sesión en https://play.google.com/work.
2. Haga clic en **Configuración de administración**.
3. En la sección **Información de la empresa**, haga clic en .
4. Haga clic en **Eliminar empresa**.
5. Haga clic en **Eliminar**.
6. En la consola de BlackBerry UEM, en la barra de menús, haga clic en **Configuración > Integración externa**.
7. Haga clic en **Conexión de dominio de Google**.
8. Haga clic en **Probar conexión**.
9. Haga clic en **Eliminar conexión**.
10. Haga clic en **Eliminar**.

Edición o prueba de la conexión de dominio de Google

Puede editar la conexión del dominio Google en BlackBerry UEM para cambiar el tipo de dominio de Google que usa para gestionar dispositivos Android Enterprise o para probar la conexión del dominio Google. Al editar o probar la conexión, no se ven afectados los dispositivos que ya están activados.

1. En la barra de menús, haga clic en **Configuración > Integración externa**.
2. Haga clic en **Conexión de dominio de Google**.
3. Haga clic en .
4. Complete una de las tareas siguientes:
   - Haga clic en **Probar conexión** para determinar el estado actual de la conexión.
   - Seleccione el tipo de dominio para gestionar los dispositivos con Android Enterprise y haga clic en **Guardar**.

Simplificación de activaciones de Windows 10

Puede utilizar una aplicación web Java de BlackBerry como un servicio de detección para simplificar el proceso de activación para los usuarios con dispositivos Windows 10. Si utiliza el servicio de detección, los usuarios no necesitan escribir una dirección de servidor durante el proceso de activación. Si elige no implementar esta aplicación web, los usuarios pueden, no obstante, activar los dispositivos Windows 10 escribiendo la dirección del servidor cuando se les solicite.

Puede utilizar diferentes sistemas operativos y herramientas de aplicación web para implementar un servicio de detección de aplicaciones web. Este tema describe los pasos de alto nivel. Consulte Implementación de un servicio de detección para simplificar las activaciones Windows 10 para ver un ejemplo de los pasos concretos que debería seguir al utilizar sistemas operativos y herramientas comunes.

Al implementar un servicio de detección de aplicación web, realice las siguientes acciones:

Paso	Acción
1	Cree un registro de host A DNS estático para el servidor de aplicaciones Java. El registro debe especificar `inscripciónempresa.<dominio_de_correo>`, donde <*dominio_de_correo*> corresponde a las direcciones de correo de los usuarios.
2	Si desea permitir que los usuarios activen dispositivos mientras están fuera de la red de la empresa, configure el equipo que aloja el servicio de detección para que lo detecte externamente a través del puerto 443.
3	Crear e instalar un certificado para proteger las conexiones TLS entre los dispositivos Windows 10 y el servicio de detección.
4	Inicie sesión en *my*Account para descargarse la herramienta de autodetección de proxy. Ejecute el archivo para extraer un archivo .war e impleméntelo en el directorio raíz del servidor de aplicaciones Java.
5	Actualice el archivo wdp.properties del servicio de detección de aplicación web para incluir una lista de ID de SRP de la empresa.

Integración de UEM con la combinación Azure Active Directory

Puede integrar BlackBerry UEM con la combinación Azure Active Directory para disfrutar de un proceso de inscripción simplificado para los dispositivos con Windows 10. Una vez configurada, los usuarios pueden inscribir sus dispositivos con UEM usando su nombre y contraseña de Azure Active Directory. La combinación de Azure Active Directory también requiere compatibilidad con Windows Autopilot, que permite que dispositivos con Windows 10 se activen automáticamente con UEM durante la configuración rápida inicial de Windows 10.

Para integrar la combinación Azure Active Directory con UEM, realice lo siguiente:

Paso	Descripción
1	Utilice el valor de la variable predeterminada %ClientlessActivationURL% en UEM para determinar las siguientes URL de modo que pueda integrar UEM con la combinación Azure Active Directory. Por ejemplo, en la pantalla de detalles del usuario de un usuario que utilice la plantilla de correo electrónico de activación predeterminada, puede hacer clic en **Ver correo electrónico de activación** para buscar el valor de %ClientlessActivationURL% en el campo del nombre del servidor de Windows 10. 1. Determinación de la URL de términos de uso de MDM. La URL utiliza la siguiente estructura: *%ClientlessActivationURL%*/azure/termsofuse Por ejemplo, si la variable %ClientlessActivationURL% se resuelve en `https://enrol.example.net/S123456789/win/mdm`, entonces, utilice `https://enrol.example.net/S123456789/win/mdm/azure/termsofuse`. 2. Determinación de la URL de detección de MDM. La URL utiliza la siguiente estructura: *%ClientlessActivationURL%*/azure/discovery Por ejemplo, si la variable %ClientlessActivationURL% se resuelve en `https://enrol.example.net/S123456789/win/mdm`, entonces, utilice `https://enrol.example.net/S123456789/win/mdm/azure/discovery`. 3. Determinación de la URI del ID de la aplicación utilizando solo el nombre del host de la variable predeterminada %ClientlessActivationURL%. Por ejemplo, si la variable %ClientlessActivationURL% se resuelve en `https://enrol.example.net/S123456789/win/mdm`, entonces, utilice `https://enrol.example.net`.
2	Integración de UEM con la combinación de Azure Active Directory.

Integración de UEM con la combinación de Azure Active Directory

Antes de empezar: Determinación de los términos de uso de MDM para utilizar la URL, la URL de detección de MDM y la URI del ID de la aplicación. Para obtener más información, consulte Integración de UEM con la combinación Azure Active Directory.

1. Inicie sesión en el portal de administración de Microsoft Azure disponible en https://portal.azure.com.
2. Desplácese hasta **Movilidad (MDM y MAM)**.
3. Haga clic en **Agregar aplicación**.
4. Haga clic en **Aplicación MDM local**. Introduzca un nombre descriptivo (por ejemplo, `BlackBerry UEM`).
5. Haga clic en **Agregar**.
6. Haga clic en la aplicación que agregó en el paso anterior para configurar sus ajustes.
7. Especifique el ámbito del usuario, **Algo** o **Todo**. Si procede, seleccione los grupos.
8. En el campo **URL de términos de uso de MDM**, especifique la URL.
9. En el campo **URL de detección de MDM**, especifique la URL.
10. Haga clic en **Guardar**.
11. Haga clic en **Configuración de la aplicación MDM local > Propiedades**.
12. En el campo **Agregar URI de ID**, especifique la URL.

13. Haga clic en **Guardar**.

Configuración de Windows Autopilot en Microsoft Azure

Para que sea compatible con la activación de dispositivos Windows Autopilot, debe realizar los siguientes pasos:

Paso	Descripción
1	Integración de UEM con la combinación de Azure Active Directory.
2	Creación de un perfil de implementación de Windows Autopilot en Azure y asígnelo a grupos de usuarios en Azure.
3	Importación de dispositivos Windows Autopilot a Azure.

Creación de un perfil de implementación de Windows Autopilot en Azure

Debe asignar un perfil de implementación de Windows Autopilot a los grupos de usuarios pertinentes en Azure para permitir que los usuarios activen sus dispositivos mediante Windows Autopilot.

1. Inicie sesión en el portal de administración de Microsoft Azure disponible en https://portal.azure.com.
2. Desplácese a **Inscripción de dispositivos > Inscripción de Windows > Perfiles de implementación de Windows Autopilot**.
3. Cree de un perfil de implementación de Windows Autopilot.
4. Introduzca un nombre y una descripción para el perfil.
5. Configure la configuración rápida inicial.
6. Asigne el perfil a los grupos de usuarios correspondientes.
7. Haga clic en **Guardar**.

Importación de dispositivos Windows Autopilot a Azure

Siga estos pasos para importar los dispositivos Windows 10 que quiera activar con Windows Autopilot.

1. Encienda el dispositivo Windows 10 para cargar la configuración rápida inicial de este.
2. Conéctese a una red Wi-Fi con conexión a Internet.
3. En el teclado, pulse **CTRL + Mayús + F3** o **CTRL + Fn + Mayús + F3.** El dispositivo se reiniciará y entrará en modo auditoría.
4. Ejecute **Windows PowerShell** como administrador.
5. Ejecute `Save-Script -Name Get-WindowsAutoPilotInfo -Path C:\Windows\Temp` para inspeccionar el script de Windows PowerShell.
6. Ejecute `Install-Script -Name Get-WindowsAutoPilotInfo` para instalar el script.
7. Ejecute `Get-WindowsAutoPilotInfo.ps1 -OutputFile C:\Windows\Temp\MyComputer.csv` para guardar la información del dispositivo en un archivo .csv.
8. Para importar un archivo .csv en Microsoft Azure , lleve a cabo las siguientes acciones:
   a) En el portal de Azure , desplácese hasta **Inscripción de dispositivos > Inscripción de Windows > Dispositivos Windows Autopilot**.

b) Haga clic en **Importar**.
c) Seleccione el archivo .csv.

9. En el diálogo **Herramienta de preparación del sistema**, realice estas acciones:
   a) En el campo **Acción de limpieza del sistema**, seleccione **Iniciar la configuración rápida (OOBE) del sistema** y anule la selección de **Generalizar**.
   b) En el campo **Opciones de apagado**, seleccione **Reiniciar**.

Implementación de un servicio de detección para simplificar las activaciones Windows 10

Los siguientes pasos describen cómo implementar el servicio de detección de aplicaciones web en el entorno descrito a continuación.

Antes de empezar: Compruebe que el siguiente software esté instalado y ejecutándose en su entorno:

- Windows Server 2012 R2
- Java JRE 1.8 o posterior
- Apache Tomcat 8 versión 8.0 o posterior

1. Configure una dirección IP estática para el equipo que alojará el servicio de detección.

   Nota: Si desea permitir que los usuarios activen dispositivos cuando están fuera de la red de la empresa, la dirección IP debe ser accesible externamente a través del puerto 443.
2. Cree un registro de host (A) de DNS para el nombre **inscripciónempresa.<*dominio_de_correo*>** que apunte a la dirección IP estática que ha configurado en el Paso 1.
3. En el directorio donde se instaló Apache Tomcat, busque el archivo server.xml para **8080** y aplique etiquetas de comentario, como se muestra en el ejemplo siguiente:

```
<!--
    <Connector port="8080" protocol="HTTP/1.1"
    connectionTimeout="20000"
    redirectPort="8443" />
    -->
```

4. Busque **server.xml** y cambie todas las instancias de **8443** a **443**.
5. Busque la sección **<Connector port="443"**, elimine las etiquetas de comentario arriba y abajo, y modifíquelo como se muestra en el ejemplo siguiente:

```
<Connector port="443" protocol="org.apache.coyote.http11.Http11NioProtocol"
    maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
    clientAuth="false" sslProtocol="TLS" keystoreFile="C:\Users
\<nombre_de_cuenta>\.keystore" />
```

6. Con la sesión iniciada como la cuenta que se especificó en el ejemplo anterior, genere un certificado ejecutando los dos comandos que se muestran en el ejemplo siguiente. Cuando se le pregunte por su nombre

y apellidos, escriba `inscripciónempresa.<dominio_de_correo_electrónico>` como se muestra en el paso siguiente:

```
C:\Archivos de programa (x86)\Java\jre1.8.0_60\bin>keytool -genkey -alias
 tomcat -keyalg RSA -keysize 2048
```

```
C:\Archivos de programa (x86)\Java\jre1.8.0_60\bin> keytool -certreq -alias
 tomcat -keyalg RSA -file <filename>.csr
```

```
C:\Archivos de programa (x86)\Java\jre1.8.0_60\bin>keytool -genkey -alias
 tomcat -keyalg RSA -keysize 2048 Introducir contraseña del almacén de claves:
 Changeit
    ¿Cuál es su nombre y apellidos?
      [Desconocido]:  inscripciónempresa.ejemplo.com
    ¿Cuál es el nombre de su unidad organizativa?
      [Desconocido]:  Departamento de TI
    ¿Cuál es el nombre de su empresa?
      [Desconocido]:  Manufacturing Co.
    ¿Cuál es el nombre de su ciudad o localidad?
      [Desconocido]:  Waterloo
    ¿Cuál es el nombre de su estado o provincia?
      [Desconocido]:  Ontario
    ¿Cuál es el código de país de dos letras de esta unidad?
      [Desconocido]:  CA
    ¿Es CN=inscripciónempresa.ejemplo.com, OU=Unidad de negocio, O=Empresa de
 ejemplo, L=Waterloo, ST=Ontario, C=CA correcto?
      [no]:  sí

    C:\Archivos de programa (x86)\Java\jre1.8.0_60\bin>keytool -certreq -alias
 tomcat -keyalg RSA -file <inscripciónempresa.ejemplo.com>.csr
    Introducir contraseña clave para <inscripciónempresa.ejemplo.com>
            (DEVOLVER si es igual que la contraseña del almacén de claves):
```

7. Envíe la solicitud de firma de certificado a una autoridad de certificación. La autoridad de certificación devolverá un archivo de extensión .p7b. Para el ejemplo anterior, la autoridad de certificación devolvería el archivo `inscripciónempresa.example.com.p7b`.
   - Si envía la solicitud de firma de certificado a una autoridad de certificación externa importante, los usuarios no deberían tener que llevar a cabo ninguna acción adicional para confiar en este certificado durante el proceso de activación.
   - Si envía la solicitud de firma de certificado a una autoridad de certificación interna, los usuarios deben instalar el certificado de la CA en el dispositivo antes de comenzar el proceso de activación.
8. Instale el certificado mediante el comando que se muestra en el ejemplo siguiente:

```
C:\Archivos de programa (x86)\Java\jre1.8.0_60\bin>keytool -import -
trustcacerts -alias tomcat -file <nombre de archivo>.p7b
```

9. Detenga Apache Tomcat.
10. Visite myAccount para descargar la herramienta de detección automática de proxy. Extraiga el contenido del archivo .zip y ejecute **W10AutoDiscovery-<*versión*>.exe**.
    El archivo .exe extraerá el archivo `W10AutoDiscovery-<versión>.war` a `C:\BlackBerry`.
11. En el directorio donde instaló Apache Tomcat, verifique la carpeta `\webapps\ROOT`. Si ya existe, elimine la carpeta `\ROOT`.
12. Cambie el nombre de `W10AutoDiscovery-<versión>.war` por `ROOT.war`. Muévalo a la carpeta `\webapps` del directorio en el que instaló Apache Tomcat.
13. Inicie Apache Tomcat.

Apache Tomcat implementará la nueva aplicación web y creará una carpeta `\webapp\ROOT`.

14. Ejecute notepad.exe como administrador. En el directorio donde ha instalado Apache Tomcat, abra `\webapps\ROOT\WEB-INF\classes\config\wdp.properties`.
15. Agregue el ID de host para el dominio de BlackBerry UEM a la línea `wdp.whitelisted.srpid` tal y como se muestra en el ejemplo que aparece a continuación. Encontrará el ID de host para el dominio de BlackBerry UEM en la consola de gestión de BlackBerry UEM. Si dispone de varios dominios de BlackBerry UEM, especifique el ID de host de cada uno. Realice las acciones siguientes:
    a) En la barra de menús, haga clic en **Configuración > Licencias > Resumen de licencias**.
    b) Haga clic en **Activar licencias**.
    c) En la lista desplegable **Método de activación de las licencias**, haga clic en **ID de host**.

    ```
    wdp.whitelisted.srpid=<ID de host>, <ID de host>, <ID de host>
    ```

16. Reinicie Apache Tomcat.

Migración de usuarios, dispositivos, grupos y otros datos desde un servidor de origen

Puede utilizar la consola de administración de BlackBerry UEM para migrar usuarios, dispositivos, grupos y otros datos desde los siguientes servidores de origen:

- BlackBerry UEM (local)
- Good Control (independiente)

Nota: Si desea migrar usuarios, dispositivos, grupos y otros datos desde un servidor de origen BES10, debe realizar la migración a BlackBerry UEM, versión 12.9. A continuación, actualizar a BlackBerry UEM, versión 12.11, después a la versión 12.14 y, posteriormente, actualizar a la versión 12.16. No se admite la migración directa desde BES10 a BlackBerry UEM versión 12.10 y posterior.

Nota: Para obtener más información sobre la migración de usuarios y dispositivos de BlackBerry Dynamics en lotes mediante archivos .csv, visite support.blackberry.com/community y lea el artículo 49442.

Para migrar usuarios, dispositivos, grupos y otros datos, realice las siguientes acciones:

Paso	Acción
1	Revise los requisitos previos de la migración.
2	Conexión con un servidor de origen.
3	Opcionalmente, migrar políticas de TI, perfiles y grupos.
4	Para las migraciones desde un servidor de origen de BlackBerry UEM con aplicaciones de BlackBerry Dynamics inscritas o desde un servidor de origen de Good Control, Migración completa de políticas y perfiles para los usuarios activados para BlackBerry Dynamics.
5	Migrar usuarios.
6	Migrar dispositivos.

Requisitos previos: Migración de usuarios, dispositivos, grupos y otros datos desde un servidor de origen

Complete los siguientes requisitos previos antes de comenzar con una migración.

Requisito previo	Detalles
Iniciar sesión	Inicie sesión en BlackBerry UEM como un administrador de seguridad. Solo un administrador debe realizar actividades de migración en un momento dado.
Comprobación de la versión de software	Para migrar los datos a BlackBerry UEM: • La instancia de BlackBerry UEM desde la que se van a migrar los datos debe corresponder a la versión 12.13 o posterior. • La instancia de Good Control (independiente) desde la que se van a migrar datos debe corresponder a la versión 5.0 o posterior.
Configuración de la conexión con el directorio de la empresa de BlackBerry UEM	Configure la conexión con el directorio de la empresa de BlackBerry UEM de destino de la misma forma en que está configurada en el origen. Por ejemplo, si el origen se ha configurado para la integración de Active Directory y se ha conectado al dominio ejemplo.com, configure BlackBerry UEM de destino para la integración de Active Directory y conéctelo al dominio ejemplo.com. **Importante:** La migración no funciona si el directorio de la empresa del servidor de destino no coincide con el directorio de la empresa del servidor de origen.
Desfragmentación de las bases de datos (BlackBerry UEM)	Desfragmente las bases de datos de origen y la base de datos de BlackBerry UEM de destino (si existe) antes de comenzar la migración. Si está migrando un gran número de usuarios, debería desfragmentar la base de datos de BlackBerry UEM de destino después de la migración de cada grupo de usuarios. Para obtener más información sobre la desfragmentación de una base de datos de Microsoft SQL Server, visite www.technet.microsoft.com para leer el artículo "Reorganizar y reconstruir índices".
BlackBerry UEM Client	Para las migraciones de aplicaciones de BlackBerry UEM Client y BlackBerry Dynamics inscritas en BlackBerry Dynamics desde una base de datos de origen de BlackBerry UEM local, debe estar instalada la versión más reciente de BlackBerry UEM Client en el dispositivo.
Comprobación del estado de las aplicaciones de BlackBerry Dynamics	Compruebe la versión de BlackBerry Dynamics SDK de todas las aplicaciones de BlackBerry Dynamics que desea migrar. Esto incluye las aplicaciones propias, las aplicaciones de BlackBerry Dynamics, las aplicaciones ISV de terceros y las aplicaciones personalizadas internas. Para las migraciones desde una base de datos de origen de BlackBerry UEM local, todas las aplicaciones de BlackBerry Dynamics deben tener BlackBerry Dynamics SDK versión 7.1 o posterior. Puede encontrar la versión de SDK en las notas de la versión de la aplicación. Para las migraciones desde una instancia (independiente) de Good Control, todas las aplicaciones deben tener BlackBerry Dynamics SDK versión 4.0. 0 o posterior. Para determinar la versión del SDK utilizada para las aplicaciones que se van a migrar, ejecute el informe de actividad del contenedor en Good Control. **Las aplicaciones de BlackBerry Dynamics que no sean compatibles con la migración se borrarán del dispositivo cuando el administrador inicie la migración.**

Requisito previo	Detalles
Comprobación de estado de los derechos de aplicaciones de BlackBerry Dynamics	Asegúrese de que: • La instancia de BlackBerry UEM de destino tiene la misma lista de derechos de aplicaciones de BlackBerry Dynamics que el servidor de origen. • A todas las cuentas de usuario migradas se les asigna la misma lista de derechos de aplicaciones de BlackBerry Dynamics que la instancia de BlackBerry UEM de destino tiene en el servidor de origen. • La delegada de autenticación es la mismo en el servidor de origen y de destino. Puede cambiar la delegada de autenticación después de la migración. • El perfil de BlackBerry Dynamics del usuario permite que BlackBerry Dynamics active la instancia de BlackBerry UEM Client si la instancia de BlackBerry UEM Client del usuario que se encuentra en el servidor de origen también lo activa BlackBerry Dynamics.  **PRECAUCIÓN:** Si faltan derechos, las aplicaciones de BlackBerry Dynamics se desactivarán después de la migración.
Revisión de ID de empresa	Las aplicaciones personalizadas solo se migran si los servidores de origen y destino tienen el mismo ID de empresa. Es posible combinar dos organizaciones. Para obtener más información, visite support.blackberry.com/community para leer el artículo 47626.
Comprobación de que los puertos necesarios no están bloqueados por un firewall ni los está utilizando otro software	Asegúrese de que los puertos 1433 (TCP) y 1434 (UDP) no están bloqueados en Microsoft SQL Server.

Conexión con un servidor de origen

Debe conectar BlackBerry UEM al servidor de origen desde el que va a migrar los datos. Puede agregar varios orígenes, pero solo un origen a la vez puede ser el origen activo.

Nota: Asegúrese de que la cuenta de la base de datos asociada a las credenciales utilizadas para iniciar sesión en la base de datos dispone de permisos de escritura.

Nota: Si ha actualizado el servidor de BlackBerry UEM de origen desde la última vez que llevó a cabo una migración, deberá eliminar y volver a crear la configuración del servidor de origen antes de llevar a cabo otra migración.

1. En la barra de menús, haga clic en **Configuración > Migración > Configuración**.
2. Haga clic en +.
3. En la lista desplegable **Tipo de origen**, seleccione el tipo de servidor de origen.
4. En función del tipo de servidor de origen seleccionado, rellene los campos tal y como se indica a continuación:

Tipo de servidor de origen	Campo	Contenido
BlackBerry UEM	Nombre para mostrar	Escriba un nombre descriptivo para el servidor de origen.
	Servidor de bases de datos	Escriba el nombre del equipo que aloja la base de datos de origen. Para ello, utilice el formato <host>\<instancia> para un puerto dinámico y el formato <host>:<puerto> para un puerto estático.
	Tipo de autenticación de la base de datos	Seleccione el tipo de autenticación que utiliza para conectarse a la base de datos de origen.
	Nombre de usuario de SQL Contraseña de SQL	Si selecciona Autenticación de SQL, en los campos Nombre de usuario de SQL y Contraseña de SQL, escriba su información de inicio de sesión para conectar con la base de datos de origen.
	Nombre de la base de datos	Escriba el nombre de la base de datos de origen.
	Tipo de autenticación de UEM de origen	Seleccione el tipo de autenticación utilizada para iniciar sesión en la consola de gestión de BlackBerry UEM de origen.
	Nombre de usuario Contraseña	Escriba la información de inicio de sesión para iniciar sesión en la consola de gestión de origen.
	Dominio	Si ha seleccionado la autenticación de Microsoft Active Directory, escriba el nombre del dominio en el que se encuentra la consola de gestión de origen.
Good Control (independiente)	Nombre para mostrar	Escriba un nombre descriptivo para el servidor de origen.
	Nombre de host de Good Control de origen (independiente)	Escriba el FQDN de la consola de gestión de Good Control.
	Certificado de Good Control de origen (independiente)	Cargue el certificado raíz de la autoridad de certificación de Good Control para establecer conexiones SSL. El archivo del certificado debe tener formato CER. Para obtener instrucciones, consulte Exportar el certificado raíz autofirmado del servidor de Good Control.

Tipo de servidor de origen	Campo	Contenido
	Nombre de usuario Contraseña	Escriba la información de inicio de sesión de la cuenta de administrador para iniciar sesión en la consola de gestión de origen. **Nota:** Estas credenciales deben corresponder a un administrador de Good Control con los derechos de acceso MANAGE_CONTAINERS y MANAGE_USERS_AND_GROUPS. La cuenta puede ser una cuenta de servicio de Good Control o una cuenta de administrador normal, siempre que la contraseña asociada a la cuenta permita acceder a la consola de gestión. No puede utilizar una cuenta de usuario de Active Directory con un identificador de hardware y sin contraseña.
	Dominio	Escriba el nombre del dominio en el que se encuentra la cuenta de administrador de la consola de gestión de origen. Puede dejar este campo en blanco si el administrador es un usuario local que no tiene un dominio.

5. Haga clic en **Guardar**.
6. Para probar la conexión entre el origen y el destino, haga clic en **Probar conexión**.
7. Haga clic en **Guardar**.

Después de terminar:

- Si desea migrar políticas de TI, perfiles y grupos, revise las prácticas recomendadas y consulte Migración de políticas de TI, perfiles y grupos desde un servidor de origen.
- Si desea migrar usuarios, revise las consideraciones y consulte Migración de usuarios desde un servidor de origen.
- Después de migrar usuarios, consulte Migración de dispositivos desde un servidor de origen.

Exportación del certificado raíz autofirmado para el servidor de Good Control

Realice la siguiente tarea si el certificado de Good Control no ha sido sustituido por ningún certificado de terceros. BlackBerry UEM confía de forma predeterminada en los certificados de proveedores de terceros, de modo que no es necesario exportar el certificado del servidor de Good Control e importarlo a BlackBerry UEM.

Nota: La siguiente tarea no es específica del navegador. Para obtener instrucciones específicas, consulte la documentación del navegador que esté utilizando.

1. En el navegador, vaya a la pantalla de inicio de sesión de cualquiera de sus servidores de Good Control. Es probable que se muestre un mensaje de error de certificado porque la CA que firmó el certificado era Good Control y el navegador no la reconoce como una CA conocida.
2. Para abrir el cuadro de diálogo Certificado, haga clic en el icono de certificado del campo URL.
3. Haga clic en **Ver certificado** o en **Información del certificado** para abrir el menú **Administración de certificados**.
4. Haga clic en la pestaña **Ruta de certificación**.

5. Seleccione el certificado raíz. El certificado raíz es el primer elemento de la jerarquía de certificados (por ejemplo, GD12345678 CA).
6. Haga clic en **Ver certificado**.
7. Haga clic en la pestaña **Detalles**.
8. Haga clic en **Copiar a archivo** o en **Exportar**.
9. Seleccione el formato **DER binario codificado X.509 (.CER)** o **Codificado en base 64 X.509 (.CER)**.
10. Introduzca una ubicación y un nombre de archivo para el certificado.
11. Haga clic en **Siguiente** o en **Guardar**.
12. Haga clic en **Finalizar**.

Consideraciones: migración de políticas de TI, perfiles y grupos desde un servidor de origen

Una migración desde un origen de BlackBerry UEM copia los siguientes elementos a la base de datos de destino:

- Políticas de TI seleccionadas
- Perfiles de correo electrónico
- Perfiles de Wi-Fi
- Perfiles VPN
- Perfiles de proxy
- Perfiles de BlackBerry Dynamics
- Perfiles de certificado de CA
- Perfiles de certificado compartido
- Recuperación de certificado
- Perfiles de credenciales de usuario
- Perfiles SCEP
- Perfiles CRL
- Perfiles OSCP
- Configuración de la autoridad de certificación (solo el conector PKI y Entrust)
- Las políticas y perfiles asociados a las políticas y los perfiles seleccionados
- Solo para la migración desde una versión local de BlackBerry UEM 12.12.1 y posteriores: ajustes de configuración de aplicaciones, perfiles de conectividad de BlackBerry Dynamics y certificados de cliente (uso de aplicaciones).

Nota: Para grupos migrados de BlackBerry UEM, las asignaciones de usuarios, funciones y de configuración de software no se migran. Debe volver a crear manualmente estas asignaciones en el servidor de destino de BlackBerry UEM.

Una migración desde un origen de Good Control (independiente) copia los siguientes elementos a la base de datos de destino:

- Conjuntos de políticas
- Perfiles de conectividad
- Grupos de aplicaciones
- Uso de aplicaciones (para los certificados)
- Certificados

BlackBerry UEM

Al migrar políticas de TI, perfiles y grupos de BlackBerry UEM a otro dominio, tenga en cuenta las siguientes directrices:

Elemento	Consideraciones
Contraseñas de políticas de TI	Si alguna de las políticas de TI de origen que se seleccionaron para los dispositivos con Android tiene una longitud mínima de la contraseña de menos de 4 o más de 16, no se pueden migrar las políticas de TI o los perfiles de BlackBerry UEM. Anule la selección o actualice la política de TI de origen y reinicie la migración.
Nombres de perfil	Después de la migración, debe asegurarse de que todos los SCEP, las credenciales de usuario, el certificado compartido y los perfiles de certificado de CA tienen nombres exclusivos. Si dos perfiles del mismo tipo tienen el mismo nombre, debe editar uno de los nombres de perfil.
Grupos de directorios	Para migrar los grupos de directorios, la base de datos de origen y la de destino deben tener solo un directorio configurado. Este directorio debe estar configurado de la misma forma en la base de datos de origen y en la de destino. Si los directorios no se configuran así, los grupos de directorios no se migran.

Aplicaciones activadas con BlackBerry Dynamics

Al migrar conjuntos de políticas de seguridad, perfiles de conectividad, grupos de aplicaciones y certificados a BlackBerry UEM, considere las siguientes directrices:

Cuando migre perfiles de conectividad y el uso de certificados a BlackBerry UEM, tenga en cuenta las siguientes directrices:

Elemento	Consideraciones
Conjuntos de políticas (solo Good Control)	Después de la migración, cada conjunto de políticas de Good Control aparece como los elementos siguientes en BlackBerry UEM: • una configuración de aplicación para cada aplicación en el conjunto de políticas • política de seguridad • política de conformidad
Perfiles de conectividad	Cuando se migran perfiles de conectividad de BlackBerry Dynamics, los valores de la pestaña Servidores de aplicaciones no se migran. Los valores se rellenan utilizando los valores predeterminados del servidor de destino de BlackBerry UEM. Cuando se migran perfiles de conectividad de BlackBerry Dynamics, algunos valores de la pestaña Infraestructura no se migran. El administrador debe editar manualmente cada perfil migrado y establecer los valores del clúster de BlackBerry Proxy y el clúster de BlackBerry Proxy secundario.

Elemento	Consideraciones
Grupos de aplicaciones (solo Good Control)	El grupo Todos se migra, pero no tiene usuarios asignados y no está relacionado con el grupo Todos los usuarios del servidor de destino de BlackBerry UEM. El administrador debe asignarlo manualmente a los usuarios si es necesario.
Aplicaciones	Si un derecho de aplicación del servidor de origen no existe en el servidor de destino, la asignación de la aplicación no se migra. El grupo de aplicaciones se migra.
Uso de certificados (BlackBerry UEM)	El uso de certificados se migra, excepto lo siguiente: • Usos de certificados que ya existen en el servidor de destino • Aplicaciones que no son de BlackBerry Dynamics • Aplicaciones personalizadas de otra empresa de Good Control

Migración de políticas de TI, perfiles y grupos desde un servidor de origen

Opcionalmente, puede migrar políticas de TI, perfiles y grupos desde un servidor de origen.

1. En la barra de menús, haga clic en **Configuración**.
2. Si tiene más de un origen configurado, en el panel izquierdo, haga clic en **Migración > Configuración** y, a continuación, seleccione el botón de opción situado junto al nombre del servidor de origen desde el que desea migrar los datos.
3. Haga clic en **Migración** > **Políticas de TI, perfiles, grupos**.
4. Haga clic en **Siguiente**.
5. Seleccione las casillas de verificación de los elementos que desea migrar.

   El nombre del servidor de origen se anexa a cada nombre de perfil y política durante la migración al destino.
6. Haga clic en **Vista previa** para revisar las políticas y los perfiles seleccionados.
7. Haga clic en **Migrar**.
8. Para configurar las políticas de TI, los perfiles y los grupos, haga clic en **Configurar políticas y perfiles de TI** y vaya a la pantalla **Políticas y perfiles**.

Después de terminar: En el servidor de destino, cree las políticas y los perfiles que no se hayan podido migrar y realice las asignaciones necesarias a los usuarios antes de migrar los dispositivos.

Después de terminar: Para obtener información específica sobre qué hacer cuando va a realizar la migración desde un servidor de origen de Good Control, consulte Migración completa de políticas y perfiles de Good Control a BlackBerry UEM.

Complete la migración de políticas y perfiles para los usuarios activados para BlackBerry Dynamics

Tras migrar usuarios, dispositivos, grupos y otros datos de Good Control a BlackBerry UEM, debe completar las siguientes tareas en el BlackBerry UEM de destino. Para obtener más información sobre dónde encontrar funciones de Good Control en BlackBerry UEM, consulte Funciones de Good Control en BlackBerry UEM.

Para restablecer las relaciones entre aplicaciones, políticas y usuarios:

- Asigne las configuraciones de aplicaciones a aplicaciones de BlackBerry Dynamics en grupos.
- Asigne los perfiles de conectividad a grupos.
- Asigne las políticas de BlackBerry Dynamics y las políticas de conformidad de Good Control migradas a usuarios.
- Configure los perfiles de anulación (perfiles de BlackBerry Dynamics y de conformidad).
- Mueva las configuraciones de archivos .json de Good Control a BlackBerry UEM (solo para migraciones de Good Control).

Para completar los perfiles de conectividad migrados:

- Introduzca la información de los servidores de aplicaciones.
- Configure los clústeres de BlackBerry Proxy en la pestaña Infraestructura.

Funciones de Good Control en BlackBerry UEM

La siguiente tabla asigna funciones de Good Control a la ubicación en BlackBerry UEM donde se puede realizar la tarea similar.

Función de Good Control	Dónde encontrarla en BlackBerry UEM
Usuarios y grupos	Haga clic en **Usuarios**.
Administradores	Haga clic en **Configuración** > **Administradores**.
Administrar aplicaciones y derechos de BlackBerry Dynamics	**Aplicaciones** y haga clic en la aplicación que desea administrar .
Limpiar, desbloquear, bloquear y administrar registros de aplicaciones de BlackBerry Dynamics	**1.** En la barra de menús, 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.** Seleccione la pestaña para el dispositivo que tiene instalada la aplicación que desea administrar. **5.** En la sección **Aplicaciones de BlackBerry Dynamics**, junto a la aplicación que desea administrar, elija el comando.
Generar claves de acceso	**1.** Haga clic en **Usuarios**. **2.** Seleccione el usuario para el que desee generar una clave de acceso. **3.** Haga clic en **Establecer contraseña de activación**. **4.** Seleccione la opción **Generación de claves de acceso de BlackBerry Dynamics**.
Administrar servicios	Haga clic en **Configuración** > **BlackBerry Dynamics** > **Servicios de la aplicación**.
Grupos de aplicaciones	Haga clic en **Grupos** > **Usuario**.
Políticas de seguridad	Haga clic en **Políticas y perfiles** > **BlackBerry Dynamics**.
Políticas de conformidad	Haga clic en **Políticas y perfiles** > **Conformidad (BlackBerry Dynamics)**.

Función de Good Control	Dónde encontrarla en BlackBerry UEM
Perfiles de aprovisionamiento	Haga clic en **Configuración** > **Valores predeterminados de activación**.
Políticas específicas de la aplicación	Haga clic en **Aplicaciones** y, a continuación, haga clic en la aplicación de BlackBerry Dynamics que desea administrar.
Agregar servidores de aplicación	Haga clic en **Políticas y perfiles** > **Conectividad (BlackBerry Dynamics)**.
Perfil de conectividad	Haga clic en **Políticas y perfiles** > **Conectividad de BlackBerry Dynamics**.
Políticas de dispositivos	Haga clic en **Políticas y perfiles** > **Política** > **Políticas de TI**.
Configuraciones del dispositivo	Haga clic en **Políticas y perfiles** > **Redes y conexiones** y seleccione los siguientes perfiles: • Wi-Fi • VPN • Proxy • Correo • Icono web • Cargas personalizadas
DEP de Apple	Haga clic en **Configuración** > **Integración externa** > **Programa de inscripción de dispositivos de Apple**.
Gestión de APNS	Haga clic en **Configuración** > **Integración externa** > **Apple Push Notification**.
Administrar autoservicio de usuario	Haga clic en **Configuración** > **Autoservicio**.
Configuración de Direct Connect	Haga clic en **Configuración** > **BlackBerry Dynamics** > **Direct Connect**.
Propiedades del servidor	Haga clic en **Configuración** > **BlackBerry Dynamics** > **Propiedades**.
Configuración de clúster de Good Proxy	Haga clic en **Configuración** > **BlackBerry Dynamics** > **Clústeres**.
Autoridades de confianza	Haga clic en **Políticas y perfiles** > **Certificados** > **Certificado de CA**. Haga clic en **Configuración** > **Integración externa** > **Autoridad de certificación**.
Definiciones de certificados	Haga clic en **Políticas y perfiles** > **Certificados** > **Credencial de usuario**. Haga clic en **Configuración** > **Integración externa** > **Autoridad de certificación**.
Certificados cargados para usuarios	Haga clic en **Usuarios**>**Todos los usuarios**>**Datos de usuario**>**Resumen**>**Política de TI y perfiles**.

Función de Good Control	Dónde encontrarla en BlackBerry UEM
Uso de las aplicaciones	**Permitir que las aplicaciones de BlackBerry Dynamics utilicen certificados de usuario y perfiles de credenciales de usuario** en las páginas de detalles de la aplicación correspondiente.
Informes	Haga clic en **Configuración** > **BlackBerry Dynamics** > **Informes**.
Trabajos del servidor	Haga clic en **Configuración** > **BlackBerry Dynamics** > **Trabajos**.

Consideraciones: Migración de usuarios desde un servidor de origen

Tenga en cuenta los siguientes aspectos al migrar usuarios a una instancia de BlackBerry UEM de destino:

Elemento	Consideraciones
Número máximo para migrar	Puede migrar un máximo de 1000 usuarios a la vez desde un origen. Si selecciona un número mayor que el número máximo de usuarios, solo el número máximo se migrará a la instancia de BlackBerry UEM de destino. El resto de usuarios se omitirá. Repita el proceso de migración tantas veces como sea necesario para migrar todos los usuarios desde el servidor de origen. **Nota:** Si se agota el tiempo de espera de BlackBerry UEM al migrar 1000 usuarios, intente migrar menos usuarios.
Dirección de correo	• Solo se pueden migrar los usuarios con una dirección de correo electrónico asociada. • No se puede migrar un usuario que ya utilice la misma dirección de correo en la instancia de BlackBerry UEM de destino. Estos usuarios no aparecen en la lista de usuarios que se van a migrar. • Si dos usuarios en la base de datos de origen tienen la misma dirección de correo , solo un usuario se muestra en la pantalla Migrar usuarios.
Dispositivo	• Tras la migración, el usuario debe utilizar la misma información de inicio de sesión para BlackBerry UEM Self-Service que la que utilizó antes de la migración.
Contraseña	Después de la migración, los usuarios locales deben cambiar sus contraseñas después de iniciar sesión en BlackBerry UEM Self-Service por primera vez. A los usuarios que no tienen permiso para acceder a BlackBerry UEM Self-Service antes de la migración no se les concede automáticamente el permiso después de la migración.
Grupos	• Puede filtrar los usuarios sin grupo asignado para incluir este conjunto de usuarios para una migración. • No puede migrar un usuario que sea propietario de un grupo de dispositivos compartidos. El usuario no aparece en la lista de usuarios que se van a migrar.

Migración de usuarios desde un servidor de origen

Se pueden migrar usuarios desde un servidor de origen a la instancia de BlackBerry UEM de destino. Los usuarios permanecen tanto en el origen como en el destino una vez completada la migración.

1. En la barra de menús, haga clic en **Configuración > Migración > Usuarios**.
2. En la pantalla **Migrar usuarios**, haga clic en **Actualizar caché**.

   La caché tarda aproximadamente 10 minutos en rellenar 1000 usuarios.

   BlackBerry UEM almacena en caché los datos de usuario para aumentar la velocidad de las capacidades de búsqueda, pero estos se migran directamente desde el origen. La actualización de la caché solo es obligatoria para el primer conjunto de usuarios migrados; después es opcional.
3. Haga clic en **Siguiente**.
4. Seleccione los usuarios que se van a migrar.

   Solo se muestran los primeros 20 000 usuarios. Busque en el nombre de usuario o la dirección de correo electrónico para localizar usuarios específicos que no estén entre los primeros 20 000. Al seleccionar todos, solo se marcan los usuarios de la primera página. Establezca el tamaño de página según el número de usuarios que desee seleccionar.

   Si se han realizado cambios en el origen una vez actualizada la caché, dichos cambios no se reflejarán en los datos de caché mostrados. No debería realizar cambios en el servidor de origen durante la migración, pero si los realiza, actualice la caché periódicamente.
5. Haga clic en **Siguiente**.
6. Asigne uno o más grupos o una política de TI y uno o más perfiles a los usuarios seleccionados.

   Para obtener más información, consulte el contenido de Administración.
7. Haga clic en **Vista previa**.
8. Haga clic en **Migrar**.

Después de terminar: Migración de dispositivos desde un servidor de origen.

Consideraciones: migración de dispositivos desde un servidor de origen

Tenga en cuenta los siguientes aspectos al migrar dispositivos a una base de datos de BlackBerry UEM de destino:

Elemento	Consideraciones
Práctica recomendada	Se recomienda migrar un único dispositivo para cada configuración única (por ejemplo, distintos grupos, políticas, configuraciones de aplicaciones, etc.) para asegurarse de que el servidor de destino se configura correctamente antes de migrar el resto de dispositivos.
Número máximo para migrar	Puede migrar un máximo de 2000 dispositivos a la vez desde un servidor de origen.
BlackBerry UEM de destino	Antes de migrar los dispositivos, verifique que BlackBerry UEM es compatible con el tipo y el SO del dispositivo.

Elemento	Consideraciones
Usuarios	• Los usuarios deben existir en el dominio de BlackBerry UEM de destino. • Debe migrar todos los dispositivos del usuario al mismo tiempo.
Dispositivos iOS gestionados con un origen de BlackBerry UEM	• Los dispositivos iOS deben tener la versión más reciente de BlackBerry UEM Client instalada. • Los dispositivos iOS asignados al perfil de bloqueo de aplicaciones no se pueden migrar porque BlackBerry UEM Client no puede abrirse para la migración. • En la configuración de la aplicación de todas las aplicaciones relevantes, desactive la casilla de verificación **Eliminar la aplicación del dispositivo cuando este se haya eliminado de BlackBerry UEM**. **Nota:** Si intenta realizar la migración sin realizar este paso, la aplicación se eliminará y se cancelará la inscripción del dispositivo de BlackBerry UEM. Sin embargo, aunque desactive esta casilla de verificación, la aplicación puede eliminarse durante la migración.
Dispositivos Android gestionados con un origen de BlackBerry UEM	• Los dispositivos Android Enterprise deben tener la versión más reciente de BlackBerry UEM Client instalada. • No se pueden migrar los dispositivos Android con un perfil de trabajo que utilice una cuenta de Google o un dominio de Google.
Dispositivos Chrome OS con un origen de BlackBerry UEM	Puede migrar los dispositivos Chrome OS.
Dispositivos Windows	No puede migrar los dispositivos Windows.
Dispositivos macOS	No puede migrar los dispositivos macOS.
Controles de MDM (BlackBerry UEM)	Los dispositivos activados con "Controles de MDM" pierden temporalmente el acceso al correo cuando la migración comience. Los servicios de correo se restauran cuando se completa la migración.
Grupos	No puede migrar un dispositivo que pertenece a un grupo de dispositivos compartidos. Estos dispositivos no aparecen en la lista de migración.

Elemento	Consideraciones
Dispositivos con BlackBerry Dynamics	**Aplicaciones de BlackBerry Dynamics** • Todas las aplicaciones de BlackBerry Dynamics compatibles con la migración se migran. **Las aplicaciones de BlackBerry Dynamics que no sean compatibles con la migración se borrarán cuando el administrador active la migración.** Estas aplicaciones se deben volver a activar en el BlackBerry UEM de destino. • Para las migraciones desde una base de datos de origen de BlackBerry UEM local, todas las aplicaciones de BlackBerry Dynamics deben tener BlackBerry Dynamics SDK versión 7.1 o posterior. • Para las migraciones desde una instancia (independiente) de Good Control, todas las aplicaciones deben tener BlackBerry Dynamics SDK versión 4.0. 0 o posterior. Para determinar la versión del SDK utilizada para las aplicaciones que se van a migrar, ejecute el informe de actividad del contenedor en Good Control. • En la pantalla Migrar dispositivos, la columna "Contenedores incompatibles" muestra el número de aplicaciones de BlackBerry Dynamics de cada dispositivo que no se pueden migrar y el número total de aplicaciones de BlackBerry Dynamics de cada dispositivo. Haga clic en el número para ver las aplicaciones de BlackBerry Dynamics que son incompatibles con la migración. • Asegúrese de que el usuario tiene los derechos de la aplicación en el BlackBerry UEM de destino. Si la aplicación no tiene el derecho, después de la migración, el usuario recibirá un mensaje que indica que la aplicación está bloqueada. • Las aplicaciones de BlackBerry Dynamics no se migran si el BlackBerry UEM de destino ya tiene aplicaciones registradas para ese usuario. • BlackBerry Access for Windows, BlackBerry Access for macOS y BlackBerry Enterprise BRIDGE no son compatibles con la migración. Cuando haya finalizado la migración, los usuarios tendrán que volver a inscribir estas aplicaciones en UEM. • Las aplicaciones personalizadas solo se migran si los servidores de origen y destino tienen el mismo ID de empresa. Es posible combinar dos organizaciones. Para obtener más información, visite support.blackberry.com/community para leer el artículo 47626. • Los dispositivos con aplicaciones de BlackBerry Dynamics activadas por varios usuarios no se deben migrar. • Es posible que las aplicaciones de BlackBerry Dynamics que se hayan bloqueado por motivos de cumplimiento o que haya bloqueado el administrador de forma remota antes de que tuviese lugar el proceso de migración dejen de funcionar después de la migración y, por tanto, puede que sea necesario volver a activarlas. Si BlackBerry UEM Client está bloqueado, el usuario no se puede migrar. • El proceso de migración no realiza un seguimiento ni garantiza la migración de BlackBerry UEM Client ni de las aplicaciones activadas en un dispositivo después de que los datos del dispositivo se hayan almacenado en caché. Los administradores deben actualizar la caché del usuario antes de cada migración. **Autenticación de dispositivos** • La aplicación delegada de autenticación debe ser la misma en el servidor de origen y en la instancia de BlackBerry UEM de destino. Puede cambiar la delegada de autenticación después de la migración. • Para las migraciones desde una instancia (independiente) de Good Control, los dispositivos con una delegada de autenticación de dispositivos de Good for Enterprise no se migran. Después de eliminar Good for Enterprise como delegada de autenticación, actualice la caché antes de continuar con la migración. Una práctica recomendada consiste en asegurarse de que al

Elemento	Consideraciones
	Administración de dispositivos • Los dispositivos que solo tengan BlackBerry Dynamics (sin BlackBerry UEM Client) pueden verse en la base de datos de origen hasta que se migren todas las aplicaciones. • Los dispositivos habilitados para BlackBerry Dynamics siempre están inscritos para BlackBerry Dynamics en el servidor de destino. • Para las migraciones desde una instancia (independiente) de Good Control, las inscripciones en MDM de Good Dynamics no se migran. El usuario debe anular la inscripción desde MDM. Si el BlackBerry UEM de destino requiere MDM, el usuario debe eliminar manualmente el perfil de MDM anterior, instalar y activar BlackBerry UEM Client, y volver a inscribir el dispositivo para MDM. **Sistema operativo** • Los dispositivos con un sistema operativo desconocido no se migran. **Sesiones de chat** • El servidor de BEMS de origen puede mantener abiertas las sesiones de chat de Connect caducadas durante un máximo de 24 horas, de modo que puede parecer de forma temporal que el usuario ha iniciado sesión en el chat desde dos dispositivos. • Los mensajes de chat de Connect no leídos se eliminan durante la migración. Los usuarios deben cerrar la sesión de Connect antes de la migración. **Usuarios** • Si un usuario tiene más de un dispositivo con aplicaciones de BlackBerry Dynamics, todos los dispositivos se seleccionan automáticamente para la migración. • No puede migrar dispositivos para el mismo usuario desde varios servidores de origen de Good Control. Puede migrar dispositivos desde varios orígenes de Good Control, pero los usuarios ya no pueden tener un dispositivo BlackBerry Dynamics en el BlackBerry UEM de destino. **Claves de desbloqueo** • Si un usuario olvida la contraseña de una aplicación de BlackBerry Dynamics después de iniciar la migración, pero antes de que el contenedor haya completado la migración, la clave de acceso de desbloqueo se debe obtener del origen de BlackBerry UEM. Después de que finalice la migración, la clave se debe obtener del BlackBerry UEM de destino. **Claves de acceso** • Después de la migración, las claves de acceso ya no se pueden generar en el servidor de origen. • El dispositivo se elimina del servidor de origen al inicio de la migración y las claves de acceso ya no se pueden generar. **Después de iniciar la migración** • Los usuarios de dispositivos iOS deben deslizar hacia arriba para cerrar las aplicaciones. • Para activar la migración en el dispositivo, una práctica recomendada consiste en abrir primero la aplicación que está configurada como la delegada de autenticación en el dispositivo. • No todas las aplicaciones aparecerán en el iniciador hasta que finalice la migración. • Después de la migración, la disposición de los iconos de las aplicaciones del iniciador se restablece a los valores predeterminados. • Los dispositivos cargan reglas de direcciones importantes, favoritos y

	Configuraciones .json (solo Good Control) • Para las migraciones desde una instancia (independiente) de Good Control, las configuraciones .json no se migran. Debido a que las configuraciones de .json son globales, al migrarlas se pueden sobrescribir las configuraciones de .json de la base de datos de destino. Asegúrese de volver a aplicar las configuraciones de .json necesarias en el servidor de destino.

Referencia rápida de migración de dispositivos

Tipo de dispositivo	Configuración/tipo de activación	Migración
Android	• Controles de MDM • BlackBerry 2FA • Privacidad del usuario • BlackBerry Dynamics (UEM a UEM)	Compatibilidad
Los dispositivos con Android Enterprise que tienen un perfil de trabajo asociado con un dominio de Google	Cualquiera	No es compatible
Los dispositivos con Android Enterprise que tienen un perfil de trabajo que no esté asociado con una cuenta de Google o un dominio de Google	Cualquiera	Compatibilidad
Los dispositivos Android Samsung Knox Workspace que tienen un perfil de trabajo asociado con una cuenta de Google y un dominio de Google	Cualquiera	No es compatible
Los dispositivos Android Samsung Knox Workspace que tienen un perfil de trabajo que no esté asociado con una cuenta de Google o un dominio de Google	Cualquiera	Compatibilidad
iOS	• Controles de MDM • Registro del dispositivo solo para BlackBerry 2FA • Dispositivos DEP que tienen BlackBerry UEM Client instalado • Privacidad del usuario • BlackBerry Dynamics (UEM a UEM)	Compatibilidad

Tipo de dispositivo	Configuración/tipo de activación	Migración
iOS	• Dispositivos DEP que no tienen BlackBerry UEM Client instalado • Inscripción de usuario	No es compatible
Windows	Cualquiera	No es compatible
macOS	Cualquiera	No es compatible

Migración de dispositivos desde un servidor de origen

Después de migrar los usuarios desde el servidor de origen a la instancia de BlackBerry UEM de destino, puede migrar los dispositivos. Los dispositivos se mueven del servidor de origen a la instancia de BlackBerry UEM de destino y dejan de estar en el origen después de la migración.

Antes de empezar:

- Antes de migrar dispositivos, compruebe que se hayan asignado los derechos y las políticas correspondientes a los usuarios que se han migrado.
- En migraciones desde BlackBerry UEM, notifique a los usuarios de dispositivos iOS que deben abrir BlackBerry UEM Client para iniciar la migración a BlackBerry UEM y que deben mantener BlackBerry UEM Client abierto hasta que se complete la migración.

1. En la barra de menús, haga clic en **Configuración > Migración > Dispositivos**.
2. En la pantalla **Migrar dispositivos**, haga clic en **Actualizar caché**.

   La caché tarda aproximadamente 10 minutos en rellenar 1000 dispositivos.

   BlackBerry UEM almacena en caché los datos de dispositivos para aumentar la velocidad de las capacidades de búsqueda, pero estos se migran directamente desde el origen. La actualización de la caché solo es obligatoria para el primer conjunto de dispositivos migrados; después es opcional.
3. Haga clic en **Siguiente**.
4. Seleccione los dispositivos que se van a migrar.

   Solo se muestran los primeros 20 000 dispositivos. Busque en el nombre de usuario o la dirección de correo electrónico para localizar usuarios específicos que no estén entre los primeros 20 000. Al seleccionar todos, solo se marcan los dispositivos de la primera página. Establezca el tamaño de página según el número de dispositivos que desee seleccionar.

   Nota: Es posible que vea menos elementos de línea que el número de dispositivos debido a que la caché se muestra por usuario y algunos usuarios pueden tener más de un dispositivo.

   Si se han realizado cambios en el origen una vez actualizada la caché, dichos cambios no se reflejarán en los datos de caché mostrados. No debería realizar cambios en el servidor de origen durante la migración, pero si los realiza, actualice la caché periódicamente.
5. Haga clic en **Vista previa**.
6. Haga clic en **Migrar**.
7. (Opcional para las migraciones desde una instancia de UEM de origen local a una instancia de UEM de destino local). Para cancelar la migración, haga clic en las casillas de verificación situadas junto a los dispositivos que desea cancelar y haga clic en ⃠.

   Si cancela la migración de un dispositivo, se debe borrar y volver a activar en el servidor de destino.

8. Para ver el estado de los dispositivos que se van a migrar, haga clic en **Migración** > **Estado**.

   En las migraciones desde Good Control, para determinar qué aplicaciones de BlackBerry Dynamics se han migrado, ejecute el informe de actividad del contenedor en Good Control.

   Asegúrese de que la configuración de Good Control se sigue ejecutando hasta que las aplicaciones delegadas de autenticación de usuario hayan completado la migración, incluso aunque se hayan migrado todos los dispositivos.

Migración de dispositivos DEP

Puede migrar los dispositivos iOS que están inscritos en el programa de inscripción de dispositivos (DEP) de Apple de una base de datos de BlackBerry UEM de origen a otra base de datos de BlackBerry UEM.

Migración de dispositivos DEP que tienen BlackBerry UEM Client instalado

Puede migrar los dispositivos iOS que están inscritos en el programa de inscripción de dispositivos de Apple (DEP) y se activan con el tipo de activación Controles de MDM.

Antes de empezar: En la configuración de la aplicación de BlackBerry UEM Client, desmarque la casilla de verificación **Eliminar la aplicación del dispositivo cuando este se haya eliminado de BlackBerry UEM**.

Nota: Si intenta realizar la migración sin realizar este paso, la aplicación se eliminará y se cancelará la inscripción del dispositivo de BlackBerry UEM. Sin embargo, aunque desactive esta casilla de verificación, la aplicación puede eliminarse durante la migración.

1. En el portal de DEP, cree un nuevo servidor virtual de MDM.
2. Conectar la instancia de BlackBerry UEM de destino al nuevo servidor de MDM virtual. Para obtener más información, consulte Configuración de BlackBerry UEM para DEP.

   Asegúrese de que el perfil de DEP de la instancia de BlackBerry UEM de destino coincida con el perfil de DEP de la instancia de BES12 o BlackBerry UEM de origen.
3. Mueva los dispositivos DEP del servidor de MDM virtual de origen al nuevo servidor MDM virtual.
4. En la consola de gestión de BlackBerry UEM, migre los dispositivos DEP de la instancia de origen a la instancia de BlackBerry UEM de destino.

Después de terminar:

Nota: Para activar la migración en el dispositivo, el usuario debe abrir primero la aplicación que está configurada como delegada de autenticación en el dispositivo.

Migre los dispositivos DEP que no tengan BlackBerry UEM Client instalado y no tengan activado BlackBerry Dynamics

Los dispositivos iOS que están inscritos en el programa de inscripción de dispositivos de Apple (DEP) y no tienen BlackBerry UEM Client instalado aparecen en la lista de dispositivos que no son compatibles para la migración.

1. En el portal de DEP, cree un nuevo servidor virtual de MDM.
2. Conecte la instancia de BlackBerry UEM de destino al nuevo servidor de MDM virtual. Para obtener más información, consulte Configuración de BlackBerry UEM para DEP.

   Asegúrese de que la instancia de BlackBerry UEM de destino tenga el mismo perfil de DEP que la instancia de origen.
3. Mueva los dispositivos DEP del servidor de MDM virtual de origen al nuevo servidor MDM virtual.
4. Realice un restablecimiento de la configuración predeterminada de fábrica de cada dispositivo DEP.
5. Reactive cada dispositivo DEP.

Configuración de BlackBerry UEM para admitir las aplicaciones de BlackBerry Dynamics

Siga las instrucciones de esta sección para configurar los ajustes de BlackBerry UEM específicos de las aplicaciones BlackBerry Proxy y BlackBerry Dynamics.

Para obtener información sobre la gestión de aplicaciones de BlackBerry Dynamics en los dispositivos de los usuarios, consulte " Gestión de aplicaciones de BlackBerry Dynamics" en el contenido de Administración.

Gestión de clústeres de BlackBerry Proxy

Cuando se instala la primera instancia de BlackBerry Proxy, BlackBerry UEM crea un clúster de BlackBerry Proxy denominado "Primero". Si solo existe un clúster, las instancias adicionales de BlackBerry Proxy se agregan al clúster de forma predeterminada. Puede crear clústeres adicionales y mover instancias de BlackBerry Proxy entre cualquiera de los clústeres disponibles. Cuando hay más de un clúster de BlackBerry Proxy disponible, no se agregan nuevas instancias a un clúster de forma predeterminada; las nuevas de clústeres se consideran no asignadas y se deben agregar a uno de los clústeres disponibles de forma manual.

1. En la consola de gestión, en la barra de menús, haga clic en **Configuración > BlackBerry Dynamics**.
2. Haga clic en **Clústeres**.
3. Lleve a cabo cualquiera de las tareas siguientes:

Tarea	Pasos
Cree un nuevo clúster de BlackBerry Proxy.	**a.** Haga clic en +. **b.** Escriba un nombre para el clúster. **c.** Haga clic en **Guardar**.
Cambie el nombre del clúster de BlackBerry Proxy.	**a.** Haga clic en un nombre de clúster. **b.** Cambie el nombre de clúster. Cada clúster debe tener un nombre único. **c.** Haga clic en **Guardar**.
Mueva una instancia de BlackBerry Proxy a un clúster de BlackBerry Proxy diferente.	**a.** En la columna **Servidores**, haga clic en el nombre de una instancia de BlackBerry Proxy. **b.** En la lista desplegable **Clúster de** BlackBerry Proxy, seleccione el clúster en el que desea agregar la instancia. **c.** Haga clic en **Guardar**.
Elimine un clúster de BlackBerry Proxy vacío.	**a.** Haga clic en × de ese clúster. **b.** Haga clic en **Eliminar**.
Establecimiento de la configuración de proxy de la aplicación para un clúster	**a.** Haga clic en **Configuración > BlackBerry Dynamics > Clústeres**. **b.** Haga clic en el nombre del clúster. **c.** Haga clic en **Anular configuración global**. Consulte Configuración de los ajustes de proxy de la aplicación BlackBerry Dynamics para obtener más información.

Tarea	Pasos
Descarga de actualizaciones del archivo PAC para todos los clústeres	• Haga clic en **Actualizar caché de PAC**
Especificación de un certificado raíz de confianza para descargar archivos PAC del servidor	**a.** Verifique que el certificado tiene el formato X.509 (*.cer y *.der) y guárdelo en una ubicación de red a la que pueda acceder desde la consola de gestión. **b.** En la barra de menús, haga clic en **Configuración > Integración externa > Certificados de confianza**. **c.** Haga clic en +, ubicado junto a **Elementos de confianza del servidor PAC**. **d.** Haga clic en **Examinar**. **e.** Seleccione el archivo de certificado que desea utilizar. **f.** Haga clic en **Abrir**. **g.** Escriba una descripción para el certificado. **h.** Haga clic en **Agregar**.
Configuración de un BlackBerry Proxy para la activación	Seleccione **Compatible con la activación** para la instancia de BlackBerry Proxy que desea usar para la activación. Se debe seleccionar al menos una instancia.

Configuración de Direct Connect utilizando reenvío de puertos

Antes de empezar:

- Configure una entrada DNS pública para cada servidor de BlackBerry Connectivity Node (por ejemplo, bp01.midominio.com, bp02.midominio.com, etc.).
- Configure el firewall externo para permitir conexiones de entrada en el puerto 17533 y para redirigir el puerto a todos los servidores de BlackBerry Connectivity Node.
- Si las instancias de BlackBerry Connectivity Nodese instalan en una DMZ, asegúrese de que los puertos correctos están abiertos entre cada BlackBerry Connectivity Node y cualquier servidor de aplicaciones al que necesiten acceder las aplicaciones de BlackBerry Dynamics (por ejemplo,Microsoft Exchange, servidores web internos y BlackBerry UEM Core).

1. En la consola de gestión, en la barra de menús, haga clic en **Configuración > BlackBerry Dynamics**.
2. Haga clic en **Direct Connect**.
3. Haga clic en una instancia de BlackBerry Proxy.
4. Para activar Direct Connect, seleccione la casilla de verificación **Activar Direct Connect**. En el campo **Nombre de host de BlackBerry Proxy**, verifique que el nombre de host sea correcto. Si la entrada DNS pública que ha creado es distinta del FQDN del servidor, especifique el FQDN externo en su lugar.
5. Repita los pasos 3 y 4 para todas las instancias de BlackBerry Proxy del clúster.

   Para permitir solo algunas instancias de BlackBerry Proxy para Direct Connect, cree un nuevo clúster de BlackBerry Proxy. Todos los servidores de un clúster deben tener la misma configuración. Para obtener más información, consulte Gestionar clústeres de BlackBerry Proxy en el contenido de Configuración.
6. Haga clic en **Guardar**.

Configuración de las propiedades de BlackBerry Dynamics

Puede configurar propiedades específicas para el uso de las aplicaciones de BlackBerry Dynamics en su empresa. Para obtener más información acerca de cada propiedad y las consecuencias de cambiar la configuración predeterminada, consulte Propiedades globales de BlackBerry Dynamics, Propiedades de BlackBerry Dynamics, Propiedades de BlackBerry Proxy y Configuración de los ajustes de proxy de la aplicación BlackBerry Dynamics. Para obtener información sobre las prácticas recomendadas para configurar las propiedades de BlackBerry Proxy, visite support.blackberry.com/community para leer el artículo 47875.

1. En la consola de gestión, en la barra de menús, haga clic en **Configuración > BlackBerry Dynamics**.
2. Lleve a cabo una de estas acciones:
   - Para configurar las propiedades globales, haga clic en **Propiedades globales**.
   - Para configurar las propiedades de una instancia de BlackBerry UEM determinada, haga clic en **Propiedades**. En la lista desplegable **Tipo de servidor**, haga clic en **Servidores de BlackBerry Control** y seleccione el servidor de BlackBerry UEM que desea configurar.
   - Para configurar las propiedades de una instancia de BlackBerry Proxy determinada, haga clic en **Propiedades**. En la lista desplegable **Tipo de servidor**, haga clic en **Servidores de BlackBerry Proxy** y seleccione el servidor de BlackBerry Proxy que desea configurar.
3. Configure las propiedades según sea necesario.
4. Haga clic en **Guardar**.

Propiedades globales de BlackBerry Dynamics

En las siguientes tablas se describen las propiedades globales de BlackBerry Dynamics que se pueden configurar.

La columna Reiniciar indica si cambiar la propiedad requiere un reinicio de BlackBerry UEM.

Nota: Si se muestra una propiedad en la consola de gestión, pero no está documentada aquí, se trata de una propiedad obsoleta que ya no está en uso.

Certificate Management

Propiedad	Descripción	Predetermi	Reiniciar
Tiempo de vida en segundos del almacén de claves de los certificados PKCS 12 de los usuarios finales individuales	La vida útil (tiempo de vida), en segundos, del almacén de claves para los certificados PKCS 12 que los usuarios de dispositivos pueden cargar para firmar mensajes de correo electrónico y para autenticación del cliente. **Nota:** Esta propiedad es de solo lectura. No puede modificarla.	86400	—

Communication

Propiedad	Descripción	Predetermi	Reiniciar
cntmgmt.internal.port	El puerto interno para el servicio de gestión de contenedores.	Nulo (predeterminado en 17317)	Sí
cntmgmt.max.conns.above.limi	El número máximo de conexiones permitidas por encima del límite establecido por la propiedad cntmgmt.max.conns.persec. **Nota:** No cambie esta configuración sin consultar al soporte técnico de BlackBerry.	3	Sí
cntmgmt.max.conns.persec	El número máximo de conexiones por segundo para la gestión de contenedores. **Nota:** No cambie esta configuración sin consultar al soporte técnico de BlackBerry.	30	Sí
cntmgmt.max.active.sessions	El número máximo de sesiones activas para la gestión de contenedores.	10000	Sí
cntmgmt.max.idle.count	El número máximo de conexiones inactivas permitidas para la gestión de contenedores. **Nota:** No cambie esta configuración sin consultar al soporte técnico de BlackBerry.	0	Sí
cntmgmt.max.read.throughput	El número máximo de operaciones de lectura simultáneas para la gestión de contenedores. **Nota:** No cambie esta configuración sin consultar al soporte técnico de BlackBerry.	500	Sí
cntmgmt.max.write.throughput	El número máximo de operaciones de escrituras simultáneas para la gestión de contenedores. **Nota:** No cambie esta configuración sin consultar al soporte técnico de BlackBerry.	500	Sí
cntmgmt.ssl.external.enable	Controla si SSL está habilitado para la gestión externa de contenedores.	Activado	Sí
cntmgmt.ssl.internal.enable	Controla si SSL está habilitado para la gestión interna de contenedores.	Activado	Sí

Contenedores duplicados

Si BlackBerry UEM identifica contenedores duplicados en dispositivos, programa trabajos por lotes para eliminarlos. Un contenedor duplicado tiene el mismo ID de usuario e ID de derecho (también conocido como el

ID de la aplicación BlackBerry Dynamics) que otro contenedor en el mismo dispositivo. Cuando un contenedor duplicado se elimina, se registra en el archivo de registro de BlackBerry UEM.

Propiedad	Descripción	Predetermi	Reiniciar
Eliminar automáticamente los contenedores duplicados en un mismo dispositivo del usuario después del aprovisionamiento	Permite especificar si BlackBerry UEM debe eliminar automáticamente los contenedores duplicados cuando se aprovisiona una nueva versión de una aplicación. Si se selecciona esta opción, tendrá prioridad sobre las demás propiedades de contenedores duplicados.	Activado	No
Habilitar trabajo para eliminar automáticamente contenedores duplicados (activado/desactivado)	Permite especificar si BlackBerry UEM debe programar automáticamente trabajos para identificar y eliminar contenedores duplicados en los dispositivos.	Activado	No
Tiempo de espera de inactividad en segundos antes de que se elimine un contenedor duplicado	El tiempo, en segundos, que un contenedor duplicado debe estar inactivo antes de que BlackBerry UEM programe un trabajo para eliminarlo.	259200	No
Frecuencia en segundos en la que se ejecutará ese trabajo para eliminar contenedores duplicados	La frecuencia, en segundos, en la que BlackBerry UEM ejecuta un trabajo para identificar y eliminar contenedores duplicados.	86400	No
Número máximo de contenedores que eliminar en un único trabajo	El número máximo de contenedores inactivos que un único trabajo puede eliminar de los dispositivos.	100	No

Delegación restringida Kerberos

Propiedad	Descripción	Predetermi	Reiniciar
Utilizar UPN explícitos	Especifique si las aplicaciones de BlackBerry Dynamics utilizan un UPN explícito o implícito a la hora de realizar la autenticación en servicios integrados con Microsoft Active Directory o Exchange ActiveSync en Office 365. En función del entorno, es posible que el Active Directory de su empresa no admita ambas opciones o que solo funcione con una de ellas.	Desactivado	No
Activar KCD (gc.krb5.enabled)	Permite especificar si BlackBerry UEM es compatible con la delegación restringida de Kerberos para aplicaciones de BlackBerry Dynamics.	Desactivad	Sí

Varios

Propiedad	Descripción	Predetermi	Reiniciar
config.command.expiry	El tiempo que BlackBerry UEM espera, en segundos, antes de volver a enviar un mensaje no confirmado.	60	Sí
config.command.retry	La frecuencia, en segundos, en la que BlackBerry UEM ejecuta una tarea para identificar y volver a enviar mensajes no confirmados. Si se establece en 0, BlackBerry UEM no ejecuta la tarea.	900	Sí
gc.entgw.report.userinfo	Permite especificar si los nombres para mostrar del usuario se notifican al NOC de BlackBerry Dynamics.	Desactivado	No
policy.compliance.interval	La frecuencia, en minutos, en la que BlackBerry UEM recupera políticas de conformidad para todos los conjuntos de políticas de BlackBerry Dynamics.	1440	Sí

Depurar los contenedores inactivos

Si BlackBerry UEM identifica contenedores inactivos en dispositivos, programa trabajos por lotes para eliminarlos. BlackBerry UEM considera que un contenedor está inactivo si no se ha conectado a BlackBerry UEM durante un periodo predeterminado de 90 días. Cuando un contenedor inactivo se elimina, se registra en el archivo de registro de BlackBerry UEM.

Nota: Este proceso no purga los contenedores que tienen una delegada de autenticación configurada.

Propiedad	Descripción	Predetermi	Reiniciar
Habilitar trabajo para eliminar automáticamente contenedores inactivos (activado/desactivado)	Permite especificar si BlackBerry UEM debe programar automáticamente trabajos para identificar y eliminar contenedores inactivos en los dispositivos.	Desactivado	No
Intervalo de inactividad del contenedor en segundos	El tiempo, en segundos, para que BlackBerry UEM considere que un contenedor está inactivo.	7776000	No
Frecuencia, en segundos, en la que se ejecutará el trabajo para eliminar contenedores inactivos	La frecuencia, en segundos, en la que BlackBerry UEM ejecuta un trabajo para identificar y eliminar contenedores inactivos.	86400	No
Número máximo de contenedores que eliminar en un único trabajo	El número máximo de contenedores inactivos que un único trabajo puede eliminar de los dispositivos.	100	No

Informes

Propiedad	Descripción	Predetermi	Reiniciar
Límite establecido para los registros devueltos en informes exportables para evitar una condición de falta de memoria.	El número máximo de líneas que se pueden incluir en un informe. El valor máximo que se puede introducir es 1 000 000.	5000	No

Política de retención de datos

Propiedad	Descripción	Predetermi	Reiniciar
Registrar operaciones de lectura en la base de datos	Si BlackBerry Control registra operaciones de lectura en la base de datos de BlackBerry Control.	Activado	Sí
Depurar trabajos del servidor	Permite especificar si BlackBerry UEM debe depurar automáticamente trabajos del servidor en intervalos regulares.	Activado	Sí
Intervalo de depuración de trabajos del servidor (en días)	Si "Depurar trabajos del servidor" está activado, la frecuencia, en días, en la que BlackBerry UEM depura trabajos del servidor.	30	Sí

Propiedades de BlackBerry Dynamics

En las siguientes tablas se describen las propiedades que se pueden configurar para cada instancia de BlackBerry UEM Core de su empresa.

Delegación restringida Kerberos

Propiedad	Descripción	Predetermi	Reiniciar
Ubicación del archivo krb5.conf en el servidor de GC (gc.krb5.config.file)	El archivo krb5.conf se utiliza para la autenticación entre dominios kerberos cuando hay una relación de confianza CAPATH con varios dominios de Kerberos.	Sin establecer	Sí
Activar modo de depuración KCD (gc.krb5.debug)	Si BlackBerry UEM registra datos de niveles de depuración.	Desactivad	Sí
Nombre completo del KDC (gc.krb5.kdc)	El FQDN del servidor que aloja el servicio del centro de distribución de claves (KDC) Kerberos.	Sin establecer	Sí
Ubicación de archivo keytab (gc.krb5.keytab.file)	La ubicación del archivo keytab de Kerberos en el ordenador que aloja BlackBerry UEM.	Sin establecer	Sí

Propiedad	Descripción	Predetermi	Reiniciar
Nombre de la cuenta de servicio en la que se ejecuta el servicio del KCD (gc.krb5.principal.name)	El nombre de usuario de la cuenta de Kerberos. No incluya el dominio o el dominio kerberos.	Sin establecer	Sí
Dominio kerberos - Active Directory (gc.krb5.realm)	El dominio kerberos de la cuenta de Kerberos.	Sin establecer	Sí

Propiedades de BlackBerry Proxy

En las siguientes tablas se describen las propiedades que se pueden configurar para cada instancia de BlackBerry Proxy de su empresa.

Propiedad	Descripción	Predeterminado	Reiniciar
gp.gps.max.sessions	Número máximo de sesiones activas.	15000	—
gp.gps.dns.server.ttl.ms	Tiempo de espera, en milisegundos, para que el servidor DNS responda.	1800000	—
gp.gps.server.flowcontrol	Permite especificar si el control de flujo está activado para el servidor.	Desactivado	—
gp.gps.tcp.keepalive	Permite especificar si TCP keepalive está activado para el servidor.	Desactivado	—
gp.gps.unalias.hostname	Para búsquedas DNS de servidores de aplicaciones, utilice el nombre de host o la dirección IP. Si selecciona esta opción, BlackBerry Proxy utiliza la búsqueda DNS inversa con la dirección IP del servidor de aplicaciones. Si no selecciona esta opción, BlackBerry Proxy utiliza el nombre de host del servidor de aplicaciones para las búsquedas DNS.	Desactivado	Sí

Propiedad	Descripción	Predeterminado	Reiniciar
gps.directconnect.suppo	Agrega y cambia paquetes de cifrado que cifran los puentes y las comunicaciones realizadas a través de BlackBerry Direct Connect. Puede optar por tener su propio servidor proxy configurado para Direct Connect y ubicarlo entre sus dispositivos de cliente y el servidor BlackBerry Proxy. Si ha agregado su propio servidor proxy, asegúrese de que los cifrados del servidor BlackBerry Proxy se corresponden con los requeridos por su propio servidor proxy. **Nota:** Todos los cifrados deben ser compatibles con Java.	TLS_ECDHE_RSA_WI	Sí
gp.directconnect. supported.protocols	Añade o cambia los protocolos de cifrado que desea que sean compatibles con el puente de conexión directa de su sistema.	TLSv1, TLSv1.1, TLSv1.2	Sí
gp.eacp.command.servic	Habilita LDAP a través de TCP para los servidores de Active Directory. Los servidores de Active Directory ofrecen el servicio LDAP a través del protocolo TCP; por tanto, los clientes encuentran un servidor LDAP mediante la consulta DNS de un registro con el formato: _ldap._tcp. DnsDomainName. Si selecciona esta opción, BlackBerry Proxy utiliza LDAP para ejecutar el comando nslookup de un nombre de host de servicio determinado. Si no selecciona esta opción, BlackBerry Proxy utiliza la búsqueda DNS inversa directamente, con el nombre de host de servicio que proporcione.	Desactivado	Sí
gc.mdc.hb.timeout	Permite especificar el tiempo de espera de latido.	0	—
gp.server.secure.ciphers	Agrega o cambia paquetes de cifrado que cifran las comunicaciones realizadas a través de un servidor BlackBerry Proxy. **Nota:** Todos los cifrados deben ser compatibles con Java.	TLS_ECDHE_RSA_WI	—
gp.server.secure. protocolos	Agrega o cambia los protocolos de cifrado que desea que sean compatibles con el servidor BlackBerry Proxy.	TLSv1, TLSv1.1, TLSv1.2	—

Configuración de los parámetros de comunicación de las aplicaciones de BlackBerry Dynamics

Puede configurar los parámetros de comunicación de las aplicaciones de BlackBerry Dynamics en el dominio de su empresa. Los parámetros de comunicación le permiten proporcionar una comunicación segura en su red mediante el protocolo de su elección. De forma predeterminada, solo se permite TLS v1.2. También puede permitir TLSv1 y v1.1. Debe seleccionar al menos un protocolo.

1. En la consola de gestión, en la barra de menús, haga clic en **Configuración > BlackBerry Dynamics**.
2. Haga clic en **Configuración de la comunicación**.
3. Ajuste la configuración según sea necesario.
4. Haga clic en **Guardar**.

Envío de los datos de aplicaciones de BlackBerry Dynamics a través de un proxy HTTP

Puede configurar BlackBerry UEM para enviar datos de aplicaciones de BlackBerry Dynamics a través de un proxy HTTP entre BlackBerry Proxy y un servidor de aplicaciones. Las aplicaciones de BlackBerry Dynamics admiten tanto con la configuración de proxy manual como los archivos PAC para conectarse a de aplicaciones. Para utilizar un archivo PAC, las aplicaciones deben haberse desarrollado con BlackBerry Dynamics SDK 7.0 o versiones posteriores. Si establece tanto la configuración manual como la configuración con un archivo PAC, el archivo PAC tendrá prioridad para las aplicaciones que sean compatibles. Las aplicaciones desarrolladas con una versión anterior de BlackBerry Dynamics SDK utilizan la configuración manual.

BlackBerry Access también es compatible con los ajustes de configuración de la aplicación de proxy manual y de archivo PAC que se aplican únicamente a la navegación con BlackBerry Access. Los ajustes de configuración de proxy para BlackBerry Access u otras aplicaciones con ajustes de proxy independientes anulan los ajustes de proxy de BlackBerry UEM. Para obtener más información, consulte la Guía de administración de BlackBerry Access.

Nota: La configuración manual de proxy también se utiliza para las conexiones con BlackBerry Dynamics NOC. El proxy debe ser capaz de acceder al puerto 443. Para obtener más información sobre los requisitos de puertos, consulte Conexiones salientes: BlackBerry UEM a BlackBerry Dynamics NOC.

Consideraciones del archivo PAC

Debe tener en cuenta las siguientes consideraciones relativas a la compatibilidad si utiliza archivos PAC con BlackBerry Proxy.

BlackBerry UEM es compatible con las siguientes directivas de archivos PAC:

- DIRECTO
- PROXY (consideradas como conexiones proxy HTTPS establecidas utilizando HTTP CONNECT)
- HTTPS (conexiones establecidas utilizando HTTP CONNECT)

BlackBerry UEM no es compatible con las siguientes directivas de archivos PAC:

- BLOCK (consideradas como DIRECT)
- SOCKS (se producirá un error de conexión)
- SOCKS4 (se producirá un error de conexión)
- SOCKS5 (se producirá un error de conexión)
- HTTP (se producirá un error de conexión)

- La directiva "NATIVE" personalizada definida por BlackBerry Access (se producirá un error de conexión)

BlackBerry UEM también tiene las siguientes limitaciones para los archivos PAC:

- La función dnsDomainIs no puede incluir los caracteres "_" ni "*".
- La función shExpMatch no puede incluir las expresiones "[0-9]", "?", "/^d" ni "d+".
- No es compatible la opción de cortar la ruta y las consultas de la URI.

Nota:

BlackBerry Proxy descarga y almacena en caché el archivo PAC para mejorar el rendimiento. La caché de PAC se actualiza cada 24 horas.

Si se publica un nuevo archivo PAC y necesita actualizar la caché inmediatamente, puede ir a **Configuración > Infraestructura > BlackBerry Router y Proxy**, expandir la sección **Configuración general** y hacer clic en **Actualizar caché de PAC**.

Configuración de los ajustes de proxy de la aplicación BlackBerry Dynamics

Puede configurar los ajustes generales de proxy de la aplicación BlackBerry Dynamics manualmente o utilizar un archivo PAC. Puede anular la configuración general de los clústeres de BlackBerry Proxy y de servidores individuales. Sin embargo, el nivel de complejidad para anular los ajustes de los servidores individuales no suele ser necesario ni recomendado.

1. Lleve a cabo una de las siguientes acciones:

Tarea	Pasos
Establecimiento de la configuración de proxy general de la aplicación	**a.** Haga clic en **Configuración > Infraestructura > BlackBerry Router y proxy**. **b.** Haga clic en **Configuración general**.
Establecimiento de la configuración de proxy de la aplicación para un clúster	**a.** Haga clic en **Configuración > BlackBerry Dynamics > Clústeres**. **b.** Haga clic en el nombre del clúster. **c.** Haga clic en **Anular configuración global**.
Establecimiento de la configuración de proxy manual de la aplicación para un servidor	**a.** Haga clic en **Configuración > Infraestructura > BlackBerry Router y proxy**. **b.** Haga clic en **Anular configuración global**. **Nota:** Los archivos PAC no son compatibles cuando se anula la configuración de proxy general para un servidor.

2. Seleccione una de las siguientes opciones:
   - **Activar proxy HTTP manual**
   - **Activar PAC**

   Los archivos PAC solo son compatibles con las conexiones a servidores de aplicaciones. Si configura ambas opciones, la configuración PAC tendrá prioridad en las conexiones a servidores de aplicaciones. Los archivos PAC solo son compatibles con las aplicaciones desarrolladas con BlackBerry Dynamics SDK 7.0 y versiones posteriores.
3. Si selecciona **Activar proxy HTTP manual**, proceda como se indica a continuación:
   a) Seleccione una de las siguientes opciones:
      - **Utilizar un proxy para conectarse únicamente a los servidores de BlackBerry Dynamics NOC**
      - **Utilizar un proxy para conectarse a todos los servidores**
      - **Utilizar un proxy para conectarse únicamente a los servidores especificados**

b) Si desea utilizar el proxy para conectarse a servidores específicos, haga clic en + para especificar más servidores.
c) En el campo **Dirección**, escriba la dirección del servidor proxy.
d) En el campo **Puerto**, escriba el número del puerto en el que escucha el servidor proxy.
e) Si el servidor proxy requiere autenticación, seleccione **Utilizar autenticación** y especifique el **Nombre de usuario**, la **Contraseña** y, si es necesario, el **Dominio** que debe utilizar la aplicación para la autenticación.

4. Si selecciona **Activar PAC**, proceda como se indica a continuación:
   a) En el campo **URL de PAC**, escriba la URL del servicio PAC.
   b) Si los servidores proxy especificados en el archivo PAC requieren autenticación, seleccione **Admitir autenticación proxy** y especifique el **Nombre de usuario**, la **Contraseña** y, si es necesario, el **Dominio** que debe utilizar la aplicación para la autenticación.

      Las credenciales de autenticación de usuario final no son compatibles para la autenticación proxy.
5. Haga clic en **Guardar**.

Conectividad y comportamiento de enrutamiento de BlackBerry Dynamics

BlackBerry UEM tiene varias opciones que permiten a los administradores controlar cómo se enruta el tráfico de BlackBerry Dynamics. El enrutamiento de las aplicaciones de BlackBerry Dynamics se ve afectado por:

- Perfil de conectividad de BlackBerry Dynamics
- Configuración del servidor proxy web de BlackBerry Proxy

  Nota: Para utilizar el servidor BlackBerry Proxy en una configuración de BlackBerry UEM Cloud, debe instalar un BlackBerry Connectivity Node local.
- Opciones específicas de la aplicación (por ejemplo, configuración del servidor proxy web de BlackBerry Access)

Antes de configurar el enrutamiento, asegúrese de que los puertos correctos están abiertos y de que tiene conectividad de red con BlackBerry Dynamics NOC. Para obtener más información, consulte Requisitos de puerto en el contenido de Planificación y Envío de datos de aplicaciones de BlackBerry Dynamics a través de un proxy HTTP.

En esta documentación solo se tratan las configuraciones que afectan al enrutamiento general. Es posible que se requiera una configuración específica de la aplicación para que las aplicaciones se conecten a servidores concretos (por ejemplo, para BlackBerry Work configurado con la URL de Microsoft Exchange Server). Revise la documentación de cada aplicación para conocer las configuraciones de aplicación que se deben aplicar.

Ruta predeterminada

De forma predeterminada, en una nueva instalación de BlackBerry UEM, todo el tráfico de las aplicaciones BlackBerry Dynamics se dirige directamente a Internet, sin ninguna configuración de servidor proxy web.

Configuración del perfil de conectividad de BlackBerry Dynamics

El único elemento configurado en el BlackBerry Dynamics perfil de conectividad predeterminado es el **Tipo de ruta de dominio predeterminado permitido**, que se establece en **Directo**.

Mediante el perfil de conectividad predeterminado de BlackBerry Dynamics , las aplicaciones BlackBerry Dynamics no pueden acceder a servidores o dominios internos. Los administradores pueden modificar el perfil de conectividad predeterminado o crear uno nuevo para permitir la conectividad a los servidores internos.

Para obtener más información, consulte Crear un perfil de conectividad de BlackBerry Dynamics.

Configuración del servidor proxy web de BlackBerry Proxy

La configuración predeterminada de los servidores BlackBerry Proxy no tiene aplicada ninguna configuración de servidor proxy web. En esta configuración, cada servidor BlackBerry Proxy intenta conectarse directamente a Internet para realizar conexiones. Esto se aplica tanto al tráfico del servidor de aplicaciones como a las conexiones de BlackBerry Dynamics NOC.

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.

El enrutamiento del 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.

Para las aplicaciones desarrolladas con BlackBerry Dynamics SDK versión 6.0 y posteriores, puede especificar los clústeres de BlackBerry Proxy por los que deberán enrutarse los datos.

Si tiene BlackBerry UEM en un entorno local, para las aplicaciones desarrolladas con una versión de BlackBerry Dynamics SDK anterior a la 6.0, seleccione la opción de distribuir todo el tráfico para enrutar todos los datos de la aplicación de BlackBerry Dynamics, independientemente del dominio o la subred, a través de BlackBerry Proxy.

Debe tener en cuenta las siguientes consideraciones a la hora de enrutar los datos a través de BlackBerry Proxy:

- 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 cómo configurar los ajustes de BlackBerry Proxy, consulte el contenido de Configuración local o el contenido de Configuración en la nube.
- BlackBerry Access se puede configurar con un archivo PAC que determina los sitios admitidos. En este caso, el archivo PAC determina los valores del proxy. Para obtener más información, consulte la Guía de administración de BlackBerry Access.

Para obtener más información, consulte Requisitos de puerto en el contenido de Planificación y Envío de datos de aplicaciones de BlackBerry Dynamics a través de un proxy HTTP.

Configuración de proxy específica de la aplicación

BlackBerry Access y algunas aplicaciones de terceros permiten la configuración del servidor proxy web a nivel de aplicación.

La configuración predeterminada de BlackBerry Access no tiene aplicada ninguna configuración de servidor proxy web. Revise la documentación de las aplicaciones BlackBerry Dynamics de terceros para conocer la configuración predeterminada de cada una.

Nota: Un servidor de aplicaciones es un servidor al que se conecta una aplicación BlackBerry Dynamics, como la dirección URL de Microsoft Exchange Server, la dirección URL de BEMS, la dirección URL de o Skype for Business o cualquier dirección URL a la que navegue BlackBerry Access. BlackBerry Dynamics NOC y el servidor BlackBerry UEM Core no son servidores de aplicaciones.

Ejemplos de escenarios de enrutamiento

Los siguientes escenarios de ejemplo reflejan las configuraciones más comunes. Si estas configuraciones no satisfacen las necesidades de su empresa o si tiene requisitos más complejos, póngase en contacto con BlackBerry Enterprise Consulting para obtener ayuda.

Escenario 1: Enrutamiento del tráfico a servidores o dominios específicos a través de BlackBerry Proxy

Esta configuración es adecuada para situaciones en las que algunas aplicaciones BlackBerry Dynamics deban tener acceso a algunos servidores de aplicaciones internos, pero el tráfico general a los servidores públicos puede seguir siendo directo.

Por ejemplo, puede enrutar las conexiones directamente a sitios públicos como google.com y microsoft.com, pero necesita un enrutamiento interno a través de BlackBerry Proxy para acceder a los servidores Microsoft Exchange Server y SharePoint internos.

En esta configuración, se asume que no se requiere una conexión de servidor proxy web a Internet, ya sea porque no se enruta ningún servidor basado en Internet a través del servidor BlackBerry Proxy o porque el propio servidor BlackBerry Proxy tiene acceso directo a Internet sin necesidad de una conexión de servidor proxy de la web.

Perfil de conectividad de BlackBerry Dynamics

1. Establezca el **Tipo de ruta de dominio permitido predeterminado** en **Directo**.
2. En **Dominios permitidos**, agregue los dominios internos que desea enrutar a través de BlackBerry Proxy y seleccione un clúster BlackBerry Proxy.
3. (Opcional) Agregue nombres de servidor específicos en **Servidores adicionales** y seleccione un clúster de BlackBerry Proxy. Esto solo es necesario si los servidores no están cubiertos ya por las reglas de **Dominios permitidos**.

Consulte Configuración del perfil de conectividad de BlackBerry Dynamics para obtener más información sobre cómo se utilizan las reglas del perfil de conectividad.

Servidor proxy web del servidor BlackBerry Proxy

No es necesario configurar el servidor proxy de la web.

Nota: Si su empresa tiene requisitos especiales para acceder a Internet desde servidores internos o requiere que todo el tráfico se enrute a través de un servidor proxy de la web, consulte los ejemplos de configuración que se muestran a continuación que incluyen configuraciones de proxy.

Servidor proxy web específico de la aplicación

No es necesaria ninguna configuración de servidor proxy de la web específico de la aplicación.

Escenario 2: enrutar todo el tráfico a través de y BlackBerry Proxy, a continuación, a través de un servidor proxy web

Esta configuración es adecuada para las empresas que necesitan que todo el tráfico de las aplicaciones de trabajo se enrute internamente. Se necesita un servidor proxy web para que los servidores internos se conecten a Internet.

Por ejemplo, las conexiones a sitios públicos como google.com y microsoft.com, así como a Microsoft Exchange Server y servidores SharePoint internos deben enrutarse internamente a través de BlackBerry Proxy.

En esta configuración, se supone que también se requiere una conexión de servidor proxy web a Internet, ya que la mayoría de las empresas que necesitan que todo el tráfico se enrute internamente también requieren que el tráfico se enrute a través de un servidor proxy web para su filtrado o supervisión.

Perfil de conectividad de BlackBerry Dynamics

1. Establezca el **Tipo de ruta de dominio permitido predeterminado** en **Clúster de BlackBerry Proxy**.

2. (Opcional) Agregue dominios internos a la lista **Dominios permitidos**. Esto no es necesario cuando el **Tipo de ruta de dominio permitido predeterminado** se ha configurado para enrutar el tráfico a través de BlackBerry Proxy.
3. (Opcional) Agregue nombres de servidor específicos en **Servidores adicionales** y seleccione un clúster de BlackBerry Proxy. Esto no es necesario cuando el **Tipo de ruta de dominio permitido predeterminado** se ha configurado para enrutar el tráfico a través de BlackBerry Proxy.
4. (Opcional) Si desea que determinados servidores estén exentos del enrutamiento predeterminado a través de BlackBerry Proxy, puede especificar dominios específicos (en **Dominios permitidos** o **Servidores adicionales**) y seleccionar **Directo**. Esto permite enrutar la mayor parte del tráfico a través de BlackBerry Proxy, excluyendo a la vez parte del tráfico (por ejemplo, para mejorar el rendimiento de determinados sitios públicos de confianza).

Consulte Configuración del perfil de conectividad de BlackBerry Dynamics para obtener más información sobre cómo se utilizan las reglas del perfil de conectividad.

Servidor proxy web del servidor BlackBerry Proxy

Dependiendo de la complejidad de su entorno, puede configurar el servidor BlackBerry Proxy para enrutar el tráfico a través de un servidor proxy web en lugar de enrutarlo directamente al servidor de destino.

Puede utilizar una configuración manual del servidor proxy web o un archivo PAC.

Nota: Puede seleccionar la configuración de proxy HTTP manual y un archivo PAC. Esto puede ser necesario para escenarios en los que el tráfico de NOC debe utilizar un servidor proxy diferente al tráfico de aplicaciones. Evite este nivel de complejidad siempre que sea posible.

Proxy HTTP manual: la configuración manual del servidor proxy web es suficiente si no hay reglas complejas que regulen qué URL deben utilizar un servidor proxy web y cuáles deben enrutarse directamente. Si todo el tráfico debe utilizar un servidor proxy web, la configuración de un servidor proxy web manual es la forma más sencilla de lograrlo.

1. Activar proxy HTTP manual:

En un entorno local	a. Haga clic en **Configuración > Infraestructura > Router y proxy de BlackBerry**. b. Expanda **Configuración general** y seleccione **Activar proxy HTTP manual**.
En un entorno de nube	a. Vaya a **Configuración > BlackBerry Dynamics > Clústeres**. b. Haga clic en el clúster que desee editar. c. Active **Anular configuración general** y seleccione **Activar proxy HTTP manual**.

2. Seleccione **Utilizar un proxy para conectarse a todos los servidores**.
3. Escriba la dirección y el puerto del servidor proxy web.

Archivo de configuración automática de proxy (PAC): si su empresa requiere reglas más complejas que determinen qué servidores deben utilizar un proxy y cuáles deben conectarse directamente, BlackBerry recomienda utilizar un archivo PAC porque es mucho más fácil de gestionar.

Por ejemplo, si desea que todas las conexiones a la red pública de Internet utilicen el servidor proxy web, pero que todos los dominios internos se conecten directamente, la práctica recomendada es utilizar un archivo PAC.

Nota: La configuración del archivo PAC no forma parte del producto BlackBerry y debe llevarla a cabo el equipo de red o proxy correspondiente de su empresa.

1. Abra la configuración de proxy:

En un entorno local	**a.** Haga clic en **Configuración > Infraestructura > Router y proxy de BlackBerry**.
En un entorno de nube	**a.** Vaya a **Configuración general > Router y proxy de BlackBerry**.

2. Expanda **Configuración general** y seleccione **Activar PAC**.
3. Introduzca la URL de PAC y la información de autenticación según sea necesario.

Servidor proxy web específico de la aplicación

No es necesaria ninguna configuración de proxy específica de la aplicación. Esta configuración asume que todo el tráfico se enruta internamente y que se utiliza una configuración de proxy manual o un archivo PAC en el servidor BlackBerry Proxy.

Escenario 3: dirija parte del tráfico internamente para la mayoría de las aplicaciones, pero configure un servidor proxy específicamente para la navegación web mediante BlackBerry Access

Esta configuración es adecuada para las empresas que requieren que el tráfico de las aplicaciones se enrute internamente, pero requieren un enrutamiento más complejo a través de un servidor proxy web específico para el tráfico del navegador.

Por ejemplo, su empresa puede decidir que es aceptable que BlackBerry Work se conecte directamente a los servidores de Microsoft Office 365. No obstante, SharePoint todavía es interno, por lo que parte del tráfico se debe enrutar a través del servidor BlackBerry Proxy. Sin embargo, la navegación está más controlada y cualquier tráfico procedente de BlackBerry Access se debe enrutar a través de un servidor proxy web para su supervisión y registro.

Esta configuración también puede incluir una configuración de servidor proxy web en el nivel del servidor BlackBerry Proxy, pero en este ejemplo se presupone que puede establecerse una conectividad directa desde el servidor BlackBerry Proxy.

Perfil de conectividad de BlackBerry Dynamics

1. Establezca el **Tipo de ruta de dominio permitido predeterminado** en **Directo**.
2. En **Dominios permitidos**, agregue todos los dominios internos que desee enrutar a través del BlackBerry Proxy y seleccione un clúster de BlackBerry Proxy.
3. (Opcional) Agregue servidores específicos que no estén incluidos en **Servidores adicionales** y seleccione un clúster de BlackBerry Proxy.

Importante: Si tiene previsto especificar un servidor proxy web alojado internamente en la configuración específica de la aplicación, debe incluir la URL del servidor proxy web en la lista Dominios permitidos o en la lista Servidores adicionales. Si la URL del servidor proxy web no está configurada para enrutar a través del servidor BlackBerry Proxy, las conexiones al servidor proxy web fallarán. Si el servidor proxy web es accesible públicamente, este paso no es necesario.

Consulte Configuración del perfil de conectividad de BlackBerry Dynamics para obtener más información sobre cómo se utilizan las reglas del perfil de conectividad.

Servidor proxy web del servidor BlackBerry Proxy

En este ejemplo se supone que los servidores BlackBerry Proxy tienen acceso directo a Internet. Si no es así, o si necesita configurar específicamente un proxy para conexiones de BlackBerry Dynamics NOC, configure un servidor proxy web según sea necesario.

Servidor proxy web específico de la aplicación

Si se necesita un servidor proxy web para una aplicación específica (por ejemplo, BlackBerry Access para navegar u otras aplicaciones de terceros), debe utilizar la configuración de la aplicación para dicha aplicación.

Nota: Consulte a otros proveedores para obtener información específica sobre la compatibilidad con un proxy específico de una aplicación y cómo configurarlo.

Si se configura un servidor proxy web específico de la aplicación, la aplicación de BlackBerry Dynamics evalúa las reglas de proxy y PAC localmente en el dispositivo antes de evaluar las reglas del perfil de conectividad de BlackBerry Dynamics. Por lo tanto, es importante que cualquier URL de proxy configurada mediante el proxy manual, o que pueda ser devuelta por el archivo PAC, se configure correctamente en el perfil de conectividad de BlackBerry Dynamics.

1. Vaya a **Aplicaciones** y, a continuación, haga clic en la aplicación que desee configurar (por ejemplo, BlackBerry Access).
2. En **Configuración de la aplicación**, cree una nueva configuración o edite una existente.
3. En BlackBerry Access, en la pestaña **Red**, seleccione **Habilitar proxy web** y **Usar configuración automática de proxy**, según sea necesario.

Para obtener más información, consulte Solucionar problemas de enrutamiento en el contenido de BlackBerry Access.

Flujo de datos de BlackBerry Dynamics

Es importante que los administradores conozcan los efectos de determinadas combinaciones de ajustes. La tabla de esta sección describe la interacción entre el perfil de conectividad de BlackBerry Dynamics y el servidor proxy HTTP configurado para el servicio BlackBerry Proxy.

Cómo evalúa BlackBerry UEM las conexiones a los hosts

El perfil de conectividad de BlackBerry Dynamics siempre se comprueba primero. Una vez que el tráfico llega al servidor BlackBerry Proxy, se evalúa la conectividad de la configuración PAC o del servidor proxy web establecida en el servidor BlackBerry Proxy. La configuración de un servidor proxy web en el servidor BlackBerry Proxy permite controlar cómo gestiona ese BlackBerry Proxy el envío de tráfico a Internet. No afecta al modo en que la aplicación de BlackBerry Dynamics del dispositivo evalúa las conexiones.

	El alojamiento en el perfil de conectividad se resuelve en BlackBerry Proxy	El alojamiento en el perfil de conectividad se resuelve en Directo	El alojamiento en el perfil de conectividad está bloqueado
Proxy/PAC = URL de proxy	Aplicación de BlackBerry Dynamics > Clúster de BlackBerry Proxy > URL del servidor proxy web > Destino	Aplicación de BlackBerry Dynamics > Destino	Contenido bloqueado por BlackBerry Dynamics SDK
Proxy/PAC = Directo	Aplicación de BlackBerry Dynamics > Clúster de BlackBerry Proxy > Destino	Aplicación de BlackBerry Dynamics > Destino	Contenido bloqueado por BlackBerry Dynamics SDK
Proxy/PAC = Bloqueo	Contenido bloqueado por el servidor proxy web	Aplicación de BlackBerry Dynamics > Destino	Contenido bloqueado por BlackBerry Dynamics SDK

Nota: Algunas aplicaciones permiten configurar un servidor proxy web o PAC específicamente para esa aplicación. Por ejemplo, BlackBerry Access permite a los administradores configurar un servidor proxy web o PAC específicamente para que BlackBerry Access lo utilice. En estos casos, la aplicación evalúa la configuración del servidor proxy web específico de la aplicación antes de evaluar el perfil de conectividad de BlackBerry Dynamics.

Para obtener más información, consulte Solucionar problemas de enrutamiento en el contenido de Administración de BlackBerry Access.

Configuración de Kerberos para aplicaciones de BlackBerry Dynamics

Las aplicaciones de BlackBerry Dynamics son compatibles con la 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.

La delegación restringida Kerberos (KCD) permite a los usuarios acceder a recursos empresariales sin necesidad de introducir sus credenciales de red. KCD utiliza vales de servicio que se cifran y descifran mediante claves que no contienen las credenciales del usuario.

Cuando se configura la *delegación*, la aplicación de BlackBerry Dynamics delega la autenticación a BlackBerry UEM para que actúe en su nombre para solicitar acceso a un recurso de trabajo. KCD *restringe* los recursos a los que se accede: los administradores pueden limitar los recursos de la red a los que se puede acceder. Esto se consigue configurando la cuenta bajo la que se ejecuta la aplicación delegada (BlackBerry UEM) como aplicación de confianza únicamente para servicios específicos.

Por ejemplo, si KCD no está configurado y una aplicación solicita un recurso como mipágina.midominio.com, la aplicación solicita al usuario credenciales. Si KCD está configurado, la infraestructura de BlackBerry Dynamics gestiona la autenticación y al usuario no se le solicitan las credenciales para el recurso.

Kerberos es una parte de Microsoft Active Directory. Antes de configurar la delegación restringida Kerberos en BlackBerry UEM, asegúrese de que su entorno Kerberos está funcionando correctamente y de que entiende las implicaciones de configurar la delegación restringida para recursos internos. Consulte la documentación pertinente de Microsoft si necesita obtener más información sobre Kerberos en general o sobre la delegación restringida.

La autenticación Kerberos PKINIT establece una confianza directa entre la aplicación de 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.

La información de esta sección es una guía. Si necesita más información sobre Kerberos y BlackBerry UEM, póngase en contacto con el equipo de soporte técnico de BlackBerry.

Dominios, dominios Kerberos y bosques

Cuando BlackBerry UEM funciona en un entorno Kerberos de *dominio único* consta de varios núcleos con configuraciones idénticas. Cuando BlackBerry UEM funciona en un entorno Kerberos de *múltiples dominios* consta de diversos núcleos con configuraciones independientes.

Un *dominio Kerberos* es un conjunto de entidades, que pueden ser dominios Kerberos de usuario o de recurso. Un dominio Kerberos de recurso es cualquier dominio Kerberos que no sea de usuario. En Kerberos, el nombre del dominio Kerberos siempre debe escribirse en mayúsculas.

Un *dominio* es un dominio de servicio de directorios. Lo más habitual es que sean de Active Directory.

Los términos dominio Kerberos y dominio son intercambiables en KCD.

Entorno de dominio Kerberos único

1. Una aplicación de BlackBerry Dynamics hace una solicitud a un servidor o servicio interno (el *destino*).

   El destino puede ser un nombre de host (nombre de servidor) o una cuenta que debe protegerse por Kerberos y BlackBerry Dynamics. Por ejemplo, si IIS se ejecuta en un servidor como servicio de red, el destino es el servidor que ejecuta IIS como red. Por otro lado, si IIS se ejecuta como un usuario (por ejemplo, IISSrvUser), el destino es ese usuario IISSrvUser.

2. El destino responde con un reto de autenticación que intercepta BlackBerry Dynamics.
3. BlackBerry Dynamics SDK envía una solicitud a BlackBerry UEM para obtener un vale de servicio para acceder al destino.
4. BlackBerry UEM autentica el usuario o la aplicación (mediante protocolos internos de BlackBerry Dynamics) y solicita un vale de servicio por cuenta del usuario (delegación) para el servicio en el destino.
5. Active Directory comprueba su política local. Si el usuario tiene permiso para acceder al recurso del destino y si el recurso del destino está permitido (restringido), Active Directory devuelve un vale de servicio a BlackBerry UEM para el recurso.
6. BlackBerry UEM envía la información necesaria del vale de servicio devuelto a BlackBerry Dynamics SDK.
7. La aplicación de BlackBerry Dynamics utiliza la información de BlackBerry UEM para completar la autenticación para el destino.

Entorno de múltiples dominios Kerberos, configuración de bosque único

En un entorno KCD de múltiples dominios, el cliente de BlackBerry Dynamics selecciona un BlackBerry UEM Core para procesar la solicitud de KCD basada en el dominio DNS del servidor de destino. Una vez que se ha determinado que el destino sea de KCD, el cliente de BlackBerry Dynamics determina la lista de servidores de BlackBerry UEM Core que se encuentran dentro del mismo dominio DNS que el destino y, a continuación, selecciona de forma aleatoria (en función de las prioridades) un BlackBerry UEM Core para procesar la solicitud.

Si no hay coincidencia de DNS (ningún servidor de BlackBerry UEM Core se encuentra en el mismo dominio DNS que el destino), el cliente hace una selección aleatoria de entre todos los servidores de BlackBerry UEM Core de la lista.

Nota: Si el recurso (por ejemplo, Microsoft Exchange) tiene un nombre de FQDN que no refleja con precisión el dominio Kerberos en el que está el recurso, BlackBerry UEM puede no ser capaz de autenticar correctamente el recurso. Por ejemplo, si el nombre de grupo de DNS del recurso es cas.domain.com, pero los servidores que se encuentran detrás de ese nombre de grupo de DNS son server1.alternatedomain.domain.com y server2.alternatedomain.domain.com, el SKD no podrá encontrar un servidor de BlackBerry UEM Core con el dominio Kerberos correcto.

El SDK compara el dominio DNS del host de destino con el dominio DNS de todos los servidores de BlackBerry UEM Core de modo que la comparación se pueda realizar sin conexión en el dispositivo en cuanto se realice la solicitud de Kerberos y sin búsquedas adicionales. Si la lista de servidores de Core del mismo dominio DNS que el destino está vacía, el SDK devuelve la lista completa de servidores. En caso contrario, utiliza la lista previamente generada. A continuación, la lista se aleatoriza y se ordena para garantizar también cumpla con las prioridades (los principales primero). SDK selecciona las dos primeras entradas e inicia la solicitud de KCD al primer servidor de Core de la lista. Si la solicitud falla, SDK envía la solicitud al segundo servidor de Core.

Para obtener más información, visite support.blackberry.com/community para leer el artículo 49304.

DNS para BlackBerry UEM y BlackBerry Connectivity Node en dominios independientes

Los servidores BlackBerry UEM y BlackBerry Connectivity Node a menudo se instalan en el mismo dominio Kerberos, pero no tiene por qué. Puede instalar el BlackBerry Connectivity Node en una DMZ o en un grupo de trabajo "de sacrificio". Si selecciona esta configuración, puede establecer algunas configuraciones de red requeridas, como las indicadas a continuación.

El funcionamiento de BlackBerry Dynamics es diferente entre un Kerberos normal (o autenticación Kerberos) y la delegación restringida Kerberos (KCD), lo que afecta a la configuración de red.

- En KCD, el servicio de BlackBerry UEM Core requiere vales de autenticación de los servidores de control de vales (el controlador de dominio) por cuenta de las aplicaciones cliente.

- En Kerberos sin delegación restringida , las aplicaciones cliente solicitan los vales y solicitan pasar a través de BlackBerry Proxy. Esto significa que BlackBerry Proxy debe poder identificar el nombre del controlador del dominio Kerberos (servidor). En el sistema de nombres de dominio (DNS), debe añadir un registro SRV en el que se especifique el servicio Kerberos que permita el reconocimiento. Este registro SRV debe estar asociado con un registro A o AAAA, no con un registro CNAME. La siguiente sintaxis es de un controlador de dominio Kerberos de un dominio de internet llamado ejemplo.com:

  ```
  _kerberos._tcp.ejemplo.com. 86400 IN SRV 0 5 88 kerberos.ejemplo.com
  ```

  Esto apunta a un servidor llamado kerberos.ejemplo.com, que escucha al puerto TCP 88 para solicitudes de Kerberos. La prioridad es 0 y el peso es 5.

Requisitos previos

- El puerto 88 del servicio de Active Directory debe ser accesible por todos los servidores de BlackBerry UEM.
- El entorno Kerberos debe incluir los siguientes componentes:
  - Servidor de Microsoft Active Directory: el servicio de directorios que autentica y autoriza a todos los usuarios y equipos asociados con su red de Windows
  - Centro de distribución de claves (KDC) de Kerberos: el servicio de autenticación del servidor de Active Directory que proporciona vales y claves de sesión a los usuarios y equipos del dominio de Active Directory
- Crear nombres principales de servicio (SPN) para todos los servicios HTTP (incluido BlackBerry Enterprise Mobility Server entre otros servicios). Debe establecer un SPN para cada recurso de destino al que quiere que los dispositivos puedan acceder. Por ejemplo:

  ```
  setspn –S HTTP/SPHOST.FQDN:PORT domain\AppPoolUser
  ```

  Para obtener más información sobre cómo crear y modificar los SPN, consulte docs.microsoft.com y lea "Registrar un nombre principal de servicio para las conexiones con Kerberos". Los propietarios de los servidores de aplicaciones o del servidor de Active Directory deberían configurar los SPN.

Para entornos Kerberos con múltiples dominios:

- Debe instalarse un servidor de BlackBerry UEM Core en cada dominio Kerberos como mínimo. BlackBerry UEM debe ubicarse en el mismo dominio Kerberos que el recurso, porque no se admite la delegación de recursos entre dominios kerberos.
- Asegúrese de que la KCD de un único dominio Kerberos funciona antes de configurar la KCD de múltiples dominios Kerberos.
- Todas las confianzas deben ser confianzas de bosque transitivas y bidireccionales.

  Importante: Garantice que haya un máximo de 5 ms de latencia entre los servidores de BlackBerry UEM Core y la base de datos de Microsoft SQL Server. Para obtener más información, consulte los requisitos de hardware de BlackBerry UEM.

Configuración de la delegación restringida Kerberos

Para realizar una configuración de dominios kerberos múltiples, empiece siempre configurando y probando un único dominio kerberos. A continuación, proceda añadiendo los demás dominios kerberos o bosques.

Nota: Si configura KCD para BlackBerry Docs, consulte Configuración de la delegación restringida Kerberos para el servicio de Docs.

Nota: Para obtener información adicional sobre el archivo keytab, visite support.blackberry.com para leer el artículo 42712.

1. Asigne la cuenta del servicio de Kerberos a un nombre principal de servicio (SPN). Abra un símbolo del sistema de administrador en el servidor Active Directory y escriba `setspn –s GCSvc/UEM_Core_equipo_host DOMINIO\Kerberos_cuenta_servicio`.

   Sustituya las variables de nombre de servidor host, dominio y cuenta de servicio con valores de tu entorno.

   Por ejemplo:

   ```
   setspn –s GCSvc/uem1.example.com example.com\kcdadmin
   ```

   Nota: La cuenta de servicio de Kerberos es el nombre de la cuenta de servicio bajo el que se configurará el servicio KCD en BlackBerry UEM(gc.krb5.nombre.principal). No es necesario que esta cuenta sea igual que la cuenta de servicio de BlackBerry UEM, pero puede serlo.
2. Cree el archivo keytab de Kerberos. Debe generar un nuevo archivo keytab y copiarlo en el servidor BlackBerry UEMcuando cambie la contraseña de la cuenta de Kerberos.

   Crear el archivo keytab Kerberos también establece la contraseña de la cuenta de Kerberos. La contraseña establecida en este comando establece la contraseña para la cuenta que especifique en el comando. Si ya ha proporcionado una contraseña, asegúrese de utilizar la misma. Si utiliza una contraseña distinta, se reseteará la contraseña. Esto incluye la contraseña de la cuenta de servicio de BlackBerry UEMsi utiliza la cuenta de servicio de UEM para crear el archivo keytab. Para crear el archivo keytab, lleve a cabo las siguientes acciones:

   a) Abra una ventana del símbolo del sistema en el servidor de KDC.
   b) Utilice el comando ktpass. Para obtener más información sobre el comando ktpass, visite docs.microsoft.com.

      ```
      ktpass -out outfilename.keytab -mapuser kerberos_account@REALM_IN_ALL_CAPS
      -princ kerberos_account@REALM_IN_UPPERCASE/ptype KRB5_NT_PRINCIPAL -pass
      kerberos_account_password
      ```

outfilename	Este es el nombre del archivo de salida.
kerberos_account	Este es el nombre de la cuenta de Kerberos.
REALM_IN_UPPERCASE	Este es el dominio Kerberos. El nombre debe estar escrito solo en mayúsculas.
-pass kerberos_account_password	Esta es la contraseña de la cuenta de Kerberos reutilizada. Si kerberos_account_password contiene caracteres especiales, como ^, ponga comillas dobles al principio y al final de la contraseña.

      Por ejemplo:

      ```
      ktpass -out outfilename.keytab -mapuser kerberos_account@REALM_IN_UPPERCASE
       -princ kerberos_account@REALM_IN_UPPERCASE /ptype KRB5_NT_PRINCIPAL -pass
       kerberos_account_password
      ```

      o

      ```
      ktpass /out outfilename.keytab /mapuser kerberos_account@REALM_IN_UPPERCASE /
      princ kerberos_account@REALM_IN_UPPERCASE /ptype KRB5_NT_PRINCIPAL /pass
       kerberos_account_password
      ```

   c) Copie el nuevo archivo keytab (en los ejemplos es kcdadmin.keytab) guardado en este directorio en el servidor de BlackBerry UEM . Importante: Si tiene varios servidores BlackBerry UEM Core configurados para

utilizar la misma cuenta de administrador de KCD, debe copiar el archivo keytab en todos los servidores BlackBerry UEM.

Puede copiar el archivo keytab en cualquier ubicación de los servidores. Por ejemplo: c:\keytab. Anote esta ubicación porque la necesitará más tarde.

3. Active la enumeración de miembros del grupo de objetos de usuarios de AD. Para obtener más información, visite docs.microsoft.com y lea "Cuentas y grupos con privilegios en Active Directory".
4. En el servidor BlackBerry UEM, configure los permisos de la cuenta de servicio de BlackBerry UEM para que pueda enviar las credenciales de usuario al sistema Kerberos. Esta es la misma cuenta que tiene asociado el nombre principal de servicio (SPN). Para configurar los permisos, realice las siguientes acciones:
   a) Abra el panel **Política de seguridad local** en la consola de Windows.
   b) En **Políticas locales**, seleccione **Asignación de derechos de usuario**, haga clic con el botón derecho en **Actuar como parte del sistema operativo** y seleccione **Propiedades**.
   c) En la ventana **Propiedades**, haga clic en **Agregar usuario o grupo**, escriba el nombre de la cuenta de servicio y haga clic en **Aceptar**.
5. Configure propiedades relacionadas con Kerberos en BlackBerry UEM.

   Puede especificar únicamente un KDC (controlador de dominio) en la configuración de BlackBerry UEM de cada servidor BlackBerry UEM Core. Esto significa que todas las llamadas de KCD al controlador de dominio irán siempre a ese único KCD. Esto podría implicar que, si ese único KCD queda fuera de servicio, todas las llamadas de KCD fallarán.

   - En Configuración > BlackBerry Dynamics > Propiedades globales, los siguientes ajustes son necesarios para activar KCD en UEM.

Propiedad	Descripción
Utilizar UPN explícitos	Active esta propiedad para hacer que BlackBerry UEM realice una autenticación utilizando el UPN explícito almacenado en Active Directory en lugar de utilizar el UPN implícito que se genera al combinar el alias de usuario y el dominio.
Activar KCD (gc.krb5.enabled)	Active esta casilla de verificación para activar KCD.

   - En Configuración > BlackBerry Dynamics > Propiedades (haga clic en el nombre del servidor), los siguientes ajustes son necesarios para activar KCD en UEM.

Propiedad	Ejemplo	Descripción
gc.krb5.kdc=<nombre_host_kcd>	Artículo UEM1.EXAMPLE.COM	El nombre de completo de KDC. Normalmente se corresponde con el FQDN de un controlador de dominio de Active Directory.
gc.krb5.keytab.file=<ubicachón_archivo_keytab>	c:/keytab/kcdadmin.keytab	La ubicación del archivo keytab. Utiliza barras diagonales y no barras invertidas en el nombre de ruta.
gc.krb5.principal.name=<cuenta_servicio_kcd>	kcdadmin@EJEMPLO.COM	El nombre de la cuenta de servicio utilizada por el servicio KCD.

Propiedad	Ejemplo	Descripción
gc.krb5.realm=<DOMINIO KERBEROS>	EXAMPLE.COM	El nombre del dominio kerberos de Active Directory El valor debe estar escrito íntegramente en mayúsculas.

6. (Opcional) Cree un archivo krb5.conf. Esto solo es necesario si hay confianza CAPATH. Consulte con su equipo de Active Directory si necesita crear este archivo.

   El archivo krb5.conf es necesario para establecer las relaciones de confianza CAPATH de varios dominios Kerberos. La ubicación del archivo krb5.conf en el servidor BlackBerry UEM debe estar especificada en la propiedad del servidor gc.krb5.config.file.

   Ejemplo de archivo krb5.conf:

```
[libdefaults] default_realm = NA.POD1.COM [realms] NA.POD1.COM = { kdc
 = pod1-na-ad.na.pod1.com } [ capaths] NA.POD1.COM = { APAC.POD2.COM =
 POD2.COM POD2.COM = POD1.COM POD1.COM = . } POD2.COM = { NA.POD1.COM =
 POD1.COM POD1.COM = . } APAC.POD2.COM = { NA.POD1.COM = POD1.COM POD1.COM =
 POD2POD2.COM POD2.COM = .}
```

Resolución de problemas y diagnósticos

Utilice los archivos de registro como ayuda para detectar problemas que su administrador del sistema puede arreglar o enviar al equipo de asistencia técnica de BlackBerry para que se investigue y resuelva. También puede consultar la base de conocimiento de BlackBerry para obtener información.

Active el registro de depuración para ver los registros.

Códigos de error de los archivos de registro de Kerberos y KCD

Con frecuencia, la información recogida en los registros del servidor de BlackBerry UEM puede explicar los errores y problemas de autenticación Kerberos y de KCD. A continuación, se ofrece un ejemplo de un registro de error de Kerberos:

```
2019-06-26T13:23:19.424-0500 - CORE {ContainerMgmtServerThread#1}
 none|none [{{externalTenantId,S12345678}}] - ERROR KRB u=
 B32F95DF-4338-499A-A06D-7EAC36852A21 while requesting KRB ServiceTicket
 for serviceClass= HTTP server= uem1.example.com port= 443 serviceName=
 httpcom.rim.platform.mdm.dynamics.kerberos.KerberosException: Failed to
 impersonate userPrincipal KCDADMIN@UEM1.EXAMPLE.COM;
             krbErrCode: 63;
             krbErrText: Fail to create credential.
```

Los dos parámetros más importantes de los mensajes de error son krbErrCode y krbErrText, ya que proporcionan una descripción de las posibles anomalías detectadas.

Para obtener una lista completa de los mensajes de error de Kerberos, visite docs.microsoft.com para leer "Mensajes de error de Kerberos y LDAP".

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 del cliente deben incluir el nombre principal del usuario (por ejemplo, user@domain.com) en el nombre alternativo del ID de objeto szOID_NT_PRINCIPAL_NAME 1.3.6.1.4.1.311.20.2.3
- 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.

Conexión de BlackBerry UEM a un conector PKI de BlackBerry Dynamics

Si desea utilizar el software PKI de su empresa para la inscripción de certificados para las aplicaciones BlackBerry Dynamics y su software PKI no es compatible con una conexión directa con BlackBerry UEM, puede configurar un conector PKI de BlackBerry Dynamics para comunicarse con su CA y vincular BlackBerry UEM con el conector PKI.

Nota: En entornos BlackBerry UEM Cloud, debe tener instalado BlackBerry Connectivity Node para permitir la comunicación de BlackBerry UEM con el conector PKI a través de BlackBerry Cloud Connector.

Un conector de PKI es un conjunto de programas Java y servicios web en un servidor backend que permite a BlackBerry UEM enviar solicitudes de certificado y recibir las respuestas de la CA. BlackBerry UEM utiliza el protocolo de gestión de certificados de usuario de BlackBerry Dynamics para comunicarse con el conector de PKI. Este protocolo se ejecuta a través de HTTPS y define los mensajes con formato JSON. Para obtener más información sobre la configuración de un conector de PKI de BlackBerry Dynamics, consulte la documentación de Protocolo de gestión de certificados de usuario y conector de PKI.

Antes de empezar: Configure un conector de PKI de BlackBerry Dynamics.

1. En la barra de menús, 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. En la sección **Certificado de confianza para el conector PKI** puede especificar el certificado que utiliza BlackBerry UEM para establecer conexiones de confianza con el conector PKI, seleccione una de las siguientes opciones:
   - **Certificado de CA de BlackBerry Control TrustStore**
   - **Certificado de CA**: si selecciona esta opción, deberá hacer clic en Examinar para seleccionar el certificado de CA de la empresa.
   - **Certificado de servidor de conector PKI**: si selecciona esta opción, deberá hacer clic en Examinar para seleccionar el certificado de servidor de conector PKI de la empresa.
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.

Integración de BlackBerry UEM con Cisco ISE

Cisco Identity Services Engine (ISE) es el software de administración de red que ofrece a las empresas la capacidad de controlar el acceso de los dispositivos a la red de trabajo (por ejemplo, permitir o denegar las conexiones VPN o Wi-Fi). Los administradores de Cisco ISE pueden crear y ejecutar políticas de acceso para asegurarse de que solo los dispositivos permitidos puedan acceder a la red de trabajo.

Puede crear una conexión entre Cisco ISE y BlackBerry UEM para que Cisco ISE pueda recuperar los datos de los dispositivos que se activan en BlackBerry UEM. Cisco ISE comprueba los datos del dispositivo para determinar si los dispositivos cumplen con las políticas de acceso. Por ejemplo:

- Cisco ISE comprueba si el dispositivo de un usuario está activado en BlackBerry UEM. Si el dispositivo no está activado, una política de acceso puede evitar que el dispositivo se conecte a los puntos de acceso VPN o a la Wi-Fi del trabajo.
- Cisco ISE comprueba si el dispositivo de un usuario cumple los requisitos de BlackBerry UEM. Si el dispositivo no cumple con los requisitos (por ejemplo, el dispositivo tiene rooting o jailbreak), una política de acceso puede evitar que el dispositivo se conecte a los puntos de acceso VPN o a la Wi-Fi del trabajo.

Los administradores de Cisco ISE pueden ver, ordenar y filtrar los datos sobre los dispositivos en la consola de gestión de Cisco ISE. Los administradores también pueden realizar las siguientes tareas de administración de dispositivos: bloquear un dispositivo, eliminar los datos de trabajo de un dispositivo o eliminar todos los datos del dispositivo.

Para integrar BlackBerry UEM con Cisco ISE, realice las siguientes acciones:

Paso	Acción
1	Verificar que el entorno de su empresa cumple los requisitos para integrar BlackBerry UEM con Cisco ISE.
2	Crear una cuenta de administrador de BlackBerry UEM que Cisco ISE pueda utilizar para obtener datos sobre los dispositivos.
3	Agregar el certificado de BlackBerry Web Services al almacén de certificados de Cisco ISE.
4	Conectar BlackBerry UEM a Cisco ISE y configurar un perfil de autorización y políticas de acceso.

Requisitos: integración de BlackBerry UEM con Cisco ISE

Elemento	Requisito
Versión Cisco ISE	BlackBerry UEM es compatible con la integración con Cisco ISE versión 1.2 y posterior.
SO compatibles	Cualquier sistema operativo compatible con BlackBerry UEM (consulte la matriz de compatibilidad), excepto los siguientes: • Windows 10 para escritorio

Elemento	Requisito
Puerto de escucha	Cisco ISE utiliza el puerto de escucha de BlackBerry Web Services predeterminado, 18084, para obtener datos sobre los dispositivos de BlackBerry UEM. Si el puerto 18084 no estaba disponible cuando BlackBerry UEM se instaló, la aplicación de configuración seleccionó otro puerto disponible con ese fin. Para verificar el valor de puerto correcto, en el archivo de registro de BlackBerry UEM Core (CORE), busque (`^/ciscoise/.*`) y registre el número de puerto que aparece justo antes de este texto.
Firewall	Si existe un firewall entre BlackBerry UEM y Cisco ISE, configure el firewall para permitir las sesiones HTTPS entre ambos sistemas.

Creación de una cuenta de administrador que Cisco ISE pueda utilizar

Cisco Identity Services Engine (ISE) requiere una cuenta de administrador de BlackBerry UEM dedicada que pueda utilizar para recuperar datos sobre los dispositivos. Puede utilizar una cuenta de administrador existente o puede crear una nueva cuenta de administrador. Debe ser una cuenta de administrador local (no a un usuario del directorio). La cuenta de administrador requiere una función con los siguientes permisos:

- Ver usuarios y dispositivos activados
- Gestionar dispositivos
- Bloquear dispositivo y establecer mensaje
- Eliminar solo los datos de trabajo
- Eliminar todos los datos del dispositivo

Las funciones de administrador de seguridad y administrador de empresa predeterminadas cuentan con estos permisos. Para crear una nueva cuenta de administrador con una función personalizada, complete los siguientes pasos con una cuenta de administrador con la función de administrador de seguridad.

Antes de empezar: Si desea crear una función personalizada para la cuenta de administrador, en la consola de gestión de BlackBerry UEM, haga clic en **Configuración > Administradores > Funciones >** . Seleccione los permisos necesarios. Haga clic en **Guardar**.

1. En la consola de gestión de BlackBerry UEM, en la barra de menús, haga clic en **Usuarios**.
2. Haga clic en **Agregar usuario**.
3. Haga clic en la pestaña **Local**.
4. Especifique el nombre, los apellidos, el nombre para mostrar, el nombre de usuario y la dirección de correo.
5. En el campo **Contraseña de la consola**, escriba una contraseña para la cuenta de administrador.
6. Seleccione la opción **No establecer contraseña de activación del dispositivo**.
7. Haga clic en **Guardar**.
8. En la barra de menús, haga clic en **Configuración**.
9. Haga clic en **Administradores > Usuarios**.
10. Haga clic en .
11. Busque y haga clic en la cuenta de usuario que ha creado.
12. En la lista desplegable **Función**, haga clic en la función personalizada que ha creado, la función de administrador de seguridad predeterminada o la función de administrador de empresa predeterminada.

13. Haga clic en **Guardar**.

Después de terminar: Adición del certificado de BlackBerry Web Services al almacén de certificados de Cisco ISE

Adición del certificado de BlackBerry Web Services al almacén de certificados de Cisco ISE

Para permitir que Cisco Identity Services Engine (ISE) se conecte a BlackBerry UEM, debe exportar el certificado de BlackBerry Web Services e importarlo al almacén de certificados de Cisco ISE. Si el dominio de BlackBerry UEM de su empresa tiene varias instancias de BlackBerry UEM, solo tiene que exportar el certificado de una instancia.

Si no dispone de una cuenta de administrador de Cisco ISE, envíe estas instrucciones al administrador de Cisco ISE.

Nota: Los pasos 3 y posteriores se basan en Cisco ISE, versión 1.4. Para obtener la documentación de Cisco ISE más reciente, visite Guías de configuración de Cisco ISE, donde podrá consultar la *Guía de administración de Cisco Identity Services Engine*.

Antes de empezar: Creación de una cuenta de administrador que Cisco ISE pueda utilizar.

1. Desde el navegador, vaya a **https://<*nombre_servidor*>:<*puerto_BlackBerry_Web_Services*>/enterprise/admin/util/ws?wsdl**, donde *<nombre_servidor>* es el FQDN del equipo que aloja el componente de BlackBerry UEM Core. El valor predeterminado de *<puerto_BlackBerry_Web_Services>* es 18084.
2. Exporte el certificado de BlackBerry Web Services y guárdelo en su escritorio. Para obtener instrucciones, consulte la documentación para el navegador que esté utilizando.

   Ejemplo: en Google Chrome, haga clic en el icono de candado situado junto a la URL. En la pestaña **Conexión**, haga clic en **Información del certificado**. En la pestaña **Detalles**, haga clic en **Copiar a archivo** y siga las instrucciones que se muestran en pantalla.
3. Inicie sesión en la consola de gestión de Cisco ISE.
4. En la barra de menús, haga clic en **Administración > Sistema > Certificados**.
5. En el panel izquierdo, haga clic en **Certificados de confianza**.
6. Haga clic en **Importar**. Vaya al certificado de BlackBerry Web Services y selecciónelo.
7. Seleccione la casilla de verificación **Confiar en la autenticación de cliente y Syslog**.
8. Seleccione la casilla de verificación **Confiar en la autenticación de Cisco Services**.
9. Haga clic en **Enviar**.

Después de terminar: Conexión de BlackBerry UEM a Cisco ISE.

Conexión de BlackBerry UEM a Cisco ISE

Si no dispone de una cuenta de administrador de Cisco Identity Services Engine (ISE), envíe estas instrucciones a un administrador de Cisco ISE, junto con la información requerida sobre BlackBerry UEM y la cuenta de administrador de BlackBerry UEM.

Nota: Los siguientes pasos se basan en Cisco ISE versión 1.4. Para obtener la documentación de Cisco ISE más reciente, visite Guías de configuración de Cisco ISE, donde podrá consultar la *Guía de administración de Cisco Identity Services Engine*.

Antes de empezar: Adición del certificado de BlackBerry Web Services al almacén de certificados de Cisco ISE.

1. Inicie sesión en la consola de gestión de Cisco ISE.

2. En la barra de menús, haga clic en **Administración > Recursos de red > External MDM**.
3. Haga clic en **Agregar**.
4. En el campo **Nombre**, escriba un nombre descriptivo para la conexión.
5. En el campo **Nombre de host o dirección IP**, escriba el FQDN o la dirección IP del dominio de BlackBerry UEM.
6. En el campo **Puerto**, escriba `18084`.

   Si el puerto 18084 no estaba disponible cuando BlackBerry UEM se instaló, la aplicación de configuración seleccionó otro puerto disponible con ese fin. Para verificar el valor de puerto correcto, en el archivo de registro de BlackBerry UEM Core (CORE), busque `(^/ciscoise/.*)` y registre el número de puerto que aparece justo antes de este texto.
7. En el campo **Nombre de usuario**, escriba el nombre de usuario de la cuenta de administrador de BlackBerry UEM.
8. En el campo **Contraseña**, escriba la contraseña de la cuenta de administrador de BlackBerry UEM.
9. En el campo **Intervalo de sondeo**, especifique con qué frecuencia (expresada en minutos) desea que Cisco ISE realice un sondeo de BlackBerry UEM para buscar datos del dispositivo. Se recomienda utilizar el valor predeterminado de 240 minutos.

   Nota: Si indica 60 minutos o menos, es posible que el rendimiento del entorno de la empresa se vea afectado significativamente. Si indica 0 minutos, Cisco ISE no realiza un sondeo de BlackBerry UEM.
10. Haga clic en la casilla de verificación **Activar**.
11. Haga clic en **Probar conexión** para verificar que Cisco ISE puede conectarse a BlackBerry UEM.
12. Haga clic en **Enviar**.

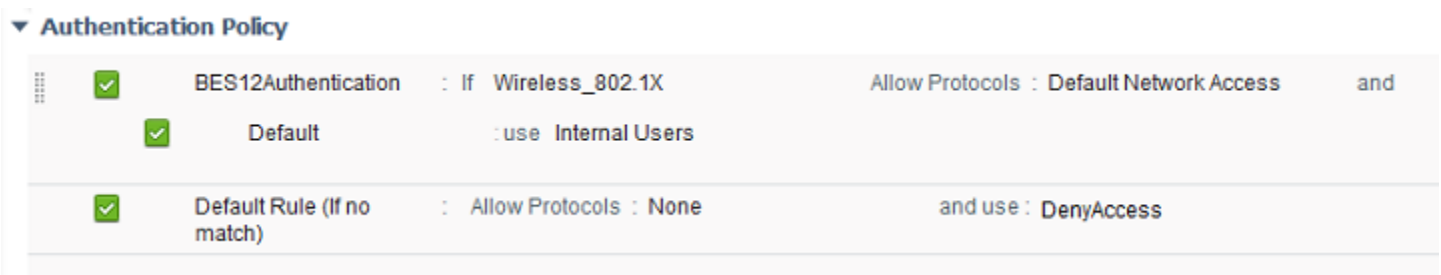
Una vez establecida la conexión, puede ver los atributos de diccionario de BlackBerry UEM en **Política > Elementos de la política > Diccionarios > Sistema > MDM > Atributos de diccionario**. Las entradas del sondeo de Cisco ISE están escritas en el archivo de registro de BlackBerry UEM Core (CORE).

Después de terminar: Realice las siguientes tareas de configuración en la consola de gestión de Cisco ISE. Para obtener las instrucciones más recientes, visite Guías de configuración de Cisco ISE para leer la *Guía de administrador de Cisco Identity Services Engine* (consulte Configuración de servidores de MDM con Cisco ISE).

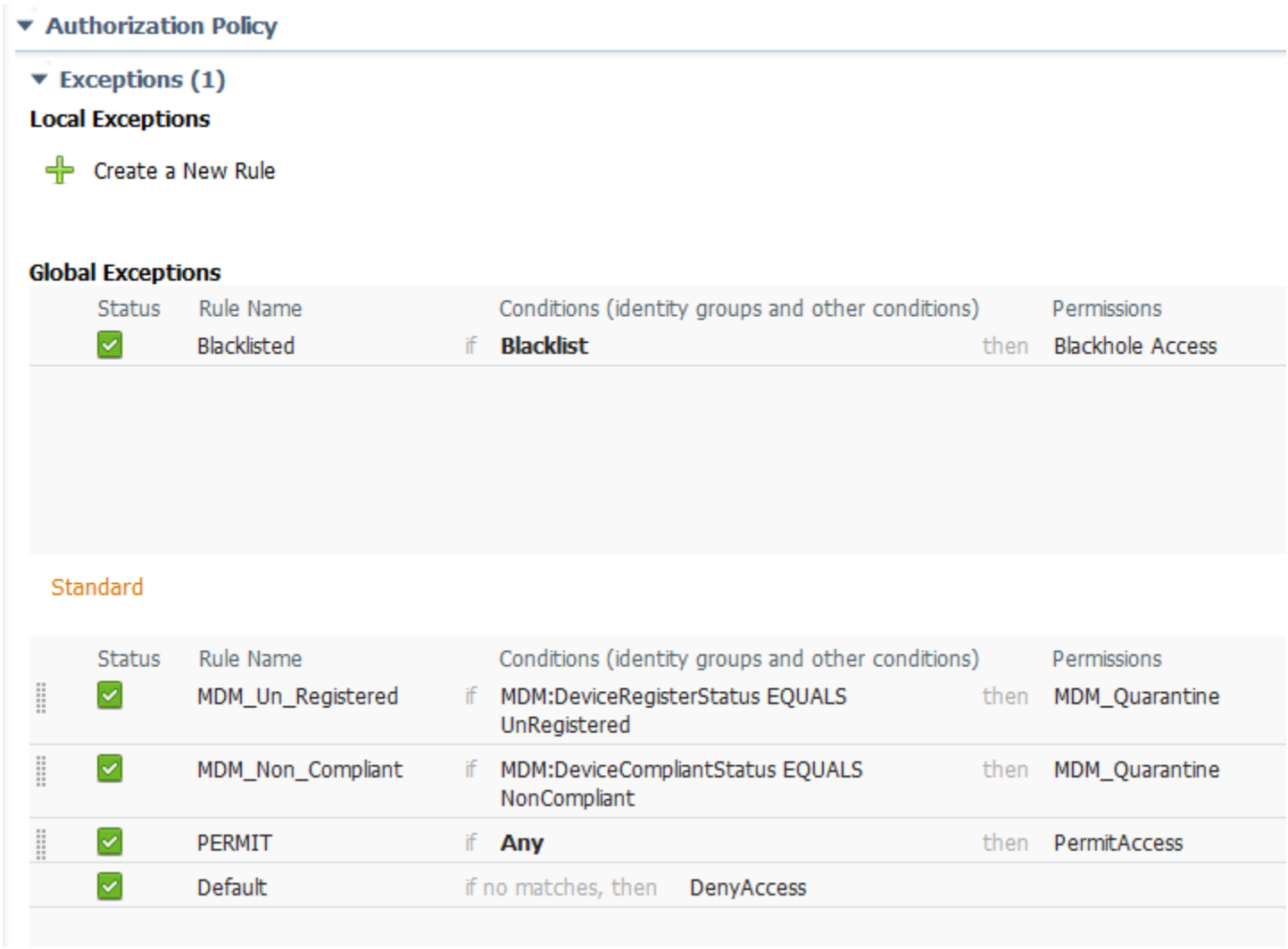
- Configure las ACL del controlador de LAN inalámbrica .
- Configure un perfil de autorización que redirija los dispositivos que no están activados en BlackBerry UEM. Para obtener más información, consulte Redirección de los dispositivos que no están activados en BlackBerry UEM.
- Configure reglas de políticas de autorización que determinen cómo Cisco ISE gestiona los dispositivos que no están activados en BlackBerry UEM ni son compatibles con BlackBerry UEM. En **Política > Conjuntos de políticas**, cree una política. Para obtener un ejemplo, consulte Ejemplo: Reglas de políticas de autorización para BlackBerry UEM.

Ejemplo: Reglas de políticas de autorización para BlackBerry UEM

Política de autenticación



Política de autorización



Administración del acceso a la red y de los controles del dispositivo con Cisco ISE

Los administradores de Cisco Identity Services Engine (ISE) pueden realizar las siguientes acciones. Para obtener más instrucciones, consulte Configuración de servidores de MDM con Cisco ISE en la *Guía de administrador de Cisco Identity Services Engine*.

Acción	Descripción
Ver datos del dispositivo	Puede ver la información sobre los dispositivos asociada a BlackBerry UEM, incluida la siguiente: • Dirección MAC: la dirección MAC exclusiva del dispositivo • Cumplimiento: si el dispositivo es compatible con BlackBerry UEM • Cifrado de disco: si los datos del dispositivo están cifrados • Inscripción: si el dispositivo está activado en BlackBerry UEM • Descodificado: si el dispositivo está descodificado o descifrado • Bloqueo de pin: si el dispositivo utiliza una contraseña • Fabricante • Modelo • Número de serie • Versión del SO
Configuración de políticas de NAC	Configure políticas de acceso que determinan si los dispositivos pueden conectarse a puntos de acceso VPN o Wi-Fi de trabajo. Por ejemplo, puede configurar una política de acceso que evite que los dispositivos no compatibles con BlackBerry UEM accedan a la red de trabajo.
Bloqueo de dispositivos	Bloquee un dispositivo iOS, Android o Windows de un usuario. Esta característica es útil si el dispositivo de un usuario tiene una ubicación incorrecta de forma temporal. BlackBerry UEM bloquea el dispositivo utilizando un comando de administración de TI. El usuario debe escribir la contraseña del dispositivo para desbloquearlo. Los usuarios de dispositivos también deben realizar esta acción a través de My Device portal.
Eliminación de los datos de trabajo	Elimine únicamente los datos y las aplicaciones de trabajo de un dispositivo, dejando los datos y las aplicaciones personales intactos. Esta característica es útil si el dispositivo de un usuario se pierde o si el usuario ya no es empleado. BlackBerry UEM elimina los datos de trabajo con un comando de administración de TI. Los usuarios de dispositivos también deben realizar esta acción a través de My Device portal.
Eliminar todos los datos	Elimine todos los datos y las aplicaciones de un dispositivo para restaurar la configuración predeterminada de fábrica. Esta característica es útil si el dispositivo de un usuario es objeto de robo o si se asigna a otro usuario. BlackBerry UEM elimina todos los datos del dispositivo con un comando de administración de TI. Los usuarios de dispositivos también deben realizar esta acción a través de My Device portal.

Para obtener más información sobre los comandos de administración de TI y los tipos de activación compatibles con los comandos de bloqueo, eliminación de datos de trabajo y eliminación de todos los datos, consulte el contenido de Administración.

Redirección de los dispositivos que no están activados en BlackBerry UEM

Si Cisco Identity Services Engine (ISE) identifica un dispositivo que intenta acceder a la red de trabajo (Wi-Fi o VPN), y el dispositivo no está activado en BlackBerry UEM, Cisco ISE abre una página de inscripción en el navegador del dispositivo que redirige al usuario a la consola de BlackBerry UEM Self-Service.

El usuario requiere una cuenta de usuario de BlackBerry UEM para iniciar sesión en BlackBerry UEM Self-Service y activar el dispositivo. Indique a los usuarios que se pongan en contacto con el administrador de BlackBerry UEM si Cisco ISE los redirige a la página de inscripción.

Para obtener más información acerca de la adición y la activación de cuentas de usuario, consulte el contenido de Administración.

Nota: Si el dispositivo del usuario se ha activado previamente con BlackBerry UEM y, a continuación, se ha desactivado, no se redirige al usuario a BlackBerry UEM Self-Service cuando este intenta acceder a la red de trabajo desde el dispositivo. Para resolver este problema, cuando elimine un dispositivo de BlackBerry UEM, elimine los datos de dicho dispositivo de Cisco ISE.

Aviso legal

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
Ground Floor, The Pearce Building, West Street,
Maidenhead, Berkshire SL6 1RL
Reino Unido

Publicado en Canadá