BlackBerry UEM

Guía de configuración

12.19

Contents

Configuración de BlackBerry UEM

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

Al realizar las tareas de configuración de esta guía, utilice la cuenta de administrador que ha creado al instalar UEM. Si crea cuentas de administrador adicionales para configurar UEM, debe asignar el rol de administrador de seguridad a las cuentas para asegurarse de que se concede el nivel de permisos adecuado.

Tarea	Local	Cloud	Descripción
Cambie los certificados predeterminados que utiliza UEM para la autenticación	√		Puede reemplazar los certificados autofirmados predeterminados que utiliza UEM para autenticar la comunicación entre los componentes y con dispositivos.
Instalación de BlackBerry Connectivity Node		√	Puede instalar y configurar BlackBerry Connectivity Node en un entorno UEM Cloud para proporcionar acceso al directorio local de la empresa y activar las funciones de conectividad seguras.
Configuración de UEM para enviar datos a través de un servidor proxy	√	√	Puede configurar UEM para enviar datos a través de un servidor proxy antes de que lleguen a BlackBerry Infrastructure. En entornos UEM Cloud, puede instalar un servidor BlackBerry Router independiente para que funcione como servidor proxy.
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 que los componentes de UEM se comuniquen con las instancias remotas de la consola de administración.
Conexión a un servidor SMTP para enviar notificaciones de correo	√		Si desea que UEM envíe mensajes de correo de activación y otras notificaciones a los usuarios, debe especificar la configuración del servidor SMTP que UEM puede utilizar.
Conexión de UEM a los directorios de la empresa	√	√	Conecte UEM a los directorios de su empresa para crear cuentas de usuario, habilitar grupos vinculados a directorios y configurar la incorporación de usuarios y la sincronización de directorios.
Conexión de UEM a Microsoft Entra ID	√	√	Conecte UEM a Entra para crear cuentas de usuario de directorio en UEM, para implementar aplicaciones iOS y Android administradas por Microsoft Intune y para configurar UEM para que admitan el acceso condicional Entra ID.

Tarea	Local	Cloud	Descripción
Registro de un certificado APN para gestionar los dispositivos iOS y macOS	√	√	Obtenga y registre un certificado APN si desea administrar y enviar datos a los dispositivos iOS y macOS.
Configuración de UEM para el programa de inscripción de dispositivos Apple	√	√	Puede utilizar la consola de administración de UEM para gestionar dispositivos iOS que su empresa haya adquirido de Apple para DEP.
Configuración de UEM para que admita dispositivos Android Enterprise	√	√	Para admitir dispositivos Android Enterprise, tiene que configurar el dominio de Google Workspace o de Google Cloud para que sea compatible con los proveedores de gestión de dispositivos móviles de terceros y configurar UEM para comunicarse con el dominio de Google Workspace o de Google Cloud.
Configuración de UEM para que admita dispositivos Android Enterprise	√	√	Para admitir dispositivos Android Management, configure Android Management en la consola Google Cloud y, a continuación, añada una conexión Android Management en UEM.
Configuración de UEM para administrar dispositivos Chrome OS	√	√	Puede configurar UEM para admitir determinadas funciones de administración de Chrome OS.
Simplificación de las activaciones de Windows 10	√	√	Puede simplificar el proceso de activación de dispositivos Windows 10 para que los usuarios no tengan que especificar una dirección de servidor.
Migración de usuarios, dispositivos, grupos y otros datos desde un servidor de origen	√	√	Puede migrar usuarios, dispositivos, grupos y otros datos desde servidores BlackBerry compatibles.
Configuración de la comunicación de red y las propiedades de las aplicaciones de BlackBerry Dynamics	√	√	Puede configurar las comunicaciones de red y otras propiedades de las aplicaciones BlackBerry Dynamics.
Integración de UEM con Cisco ISE	√		Puede crear una conexión con Cisco ISE para que pueda recuperar los datos del dispositivo desde UEM y aplicar las políticas de control de acceso a la red.
Configuración de la VPN con Knox StrongSwan para entornos de sitio oscuro de UEM	√		En un entorno de sitio oscuro de UEM, debe configurar el acceso VPN para que los dispositivos Samsung Knox puedan acceder a los servidores y recursos internos.

Cambio de los certificados que BlackBerry UEM utiliza para la autenticación

Cuando se instala BlackBerry UEM local, 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.

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 de firma de perfil de Apple	Es el certificado que 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 autoridad de certificación, asegúrese de que el certificado raíz de la autoridad de certificación esté instalado en los dispositivos iOS de los usuarios antes de la activación.
Certificado SSL para consolas	Es el certificado SSL que la consola de administración y UEM Self-Service utilizan para autenticar los exploradores. Si configura la alta disponibilidad, el certificado debe tener el nombre del dominio de UEM. Puede encontrar el nombre de dominio en la consola de administración, en **Configuración > Infraestructura > Instancias.**
Certificados SSL para BlackBerry Web Services	Es el certificado SSL que BlackBerry Web Services utiliza para autenticar las aplicaciones que usan las API de BlackBerry Web Services para gestionar UEM. Si configura la alta disponibilidad, el certificado debe tener el nombre del dominio de UEM. Puede encontrar el nombre de dominio en la consola de administración, en **Configuración > Infraestructura > Instancias.**
Certificado SSL para aplicaciones de BlackBerry Dynamics	Un certificado SSL que BlackBerry Dynamics Launcher utiliza para establecer un canal de comunicación seguro con UEM. Las aplicaciones de BlackBerry Dynamics que incluyen el BlackBerry Dynamics Launcher integrado pueden presentar el certificado a UEM para autenticarse en el servidor.
Certificado de gestión de aplicaciones	Es el certificado SSL que se utiliza para la autenticación entre las aplicaciones de UEM y BlackBerry Dynamics. El certificado de autoridad de certificación raíz se almacena en la lista de certificados de autoridades de certificación 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 UEM inserte el certificado en todas las aplicaciones de BlackBerry Dynamics, será necesario volver a activar las aplicaciones que no hayan recibido el certificado.

Certificado	Descripción
Certificado para Direct Connect	Este es el certificado SSL que se utiliza para la autenticación entre un servidor BlackBerry Proxy configurado para aplicaciones BlackBerry Dynamics Direct Connect y BlackBerry Dynamics en dispositivos. Al actualizar este certificado, la nueva versión siempre se enviará a los dispositivos a través de una conexión Direct Connect que no es de BlackBerry Dynamics. 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 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.
Certificado para servidores de BlackBerry Dynamics	Es el certificado SSL que autentica las conexiones entre UEM y BlackBerry Proxy.

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 UEM y BlackBerry Dynamics podría verse interrumpida. Planifique y pruebe los cambios de certificados con cuidado.

Consideración	Detalles
Añadir nuevos certificados a un equipo periférico	Si ha añadido certificados de BlackBerry Dynamics a equipos periféricos de su red, añada el nuevo certificado al equipo periférico antes de añadirlo a UEM.
Utilizar las versiones más recientes de las aplicaciones BlackBerry Dynamics	Si va a sustituir el certificado de BlackBerry Dynamics para la administración de aplicaciones o Direct Connect, asegúrese de que los usuarios utilicen la última versión de las aplicaciones de BlackBerry Dynamics antes de sustituir el certificado.
Las aplicaciones de BlackBerry Dynamics debe estar abiertas para recibir un certificado	Un usuario debe abrir una aplicación de BlackBerry Dynamics en su dispositivo para que reciba un certificado de 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 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.

Consideración	Detalles
Comprobar que BlackBerry Connectivity Node sea accesible	Si cualquiera de las instancias de BlackBerry Proxy no está accesible para 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.
Programar cambios de certificado	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.

Cambio de un certificado de BlackBerry UEM

Antes de empezar:

- Revise la Consideraciones para cambiar los certificados de BlackBerry Dynamics.
- Obtenga un certificado firmado por una CA de confianza. El certificado debe estar en un formato de almacén de claves (.pfx, .pkcs12) y debe estar cifrado con el tipo de cifrado TripleDES-SHA1.

1. En la barra de menús de la consola de administración, haga clic en **Configuración > Infraestructura > Certificados del servidor**.
2. En las pestañas **Certificados de servidor** o **Certificados de BlackBerry Dynamics**, en la sección del certificado que desea reemplazar, haga clic en **Ver detalles**.
3. Haga clic en **Sustituir certificado**.
4. Haga clic en **Examinar**. Navegue al archivo de certificado y selecciónelo.
5. En el campo **Contraseña de cifrado** o **Contraseña**, escriba una contraseña.
6. Haga clic en **Sustituir**.

Después de terminar:

- Si ha sustituido alguno de los certificados de la pestaña Certificados de servidor, reinicie el servicio UEM Core en todos 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 desmarcar 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. Solo se puede desmarcar la casilla de verificación **Confiar en la CA de BlackBerry Dynamics** 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 estén actualizadas y, a continuación, indique a los usuarios que vuelvan a activar las aplicaciones.

Instalación de BlackBerry Connectivity Node para conectarse a los recursos detrás del firewall de la empresa

BlackBerry Connectivity Node es un conjunto de componentes que puede instalar en un equipo específico para activar funciones adicionales para BlackBerry UEM Cloud. Los siguientes componentes se incluyen en BlackBerry Connectivity Node.

Componente	Finalidad
BlackBerry Cloud Connector	BlackBerry Cloud Connector permite a UEM Cloud acceder al directorio local de la empresa. Puede crear cuentas de usuario de directorio en UEM buscando los datos del usuario en el directorio de la empresa e importándolos. Los datos del usuario se sincronizan con el directorio según la programación que configure. Si desea utilizar SCEP, UEM Cloud debe poder acceder al directorio de su empresa. Los usuarios de directorio pueden utilizar las credenciales para acceder a BlackBerry UEM Self-Service. Si asigna una función administrativa a los usuarios del directorio, dichos usuarios pueden utilizar también sus credenciales de directorio para iniciar sesión en la consola de gestión. BlackBerry Cloud Connector también permite que un conector de PKI envíe certificados a aplicaciones de BlackBerry Dynamics.
BlackBerry Proxy	BlackBerry Proxy mantiene una conexión entre su empresa y BlackBerry Dynamics NOC que permite a las aplicaciones BlackBerry Dynamics comunicarse de forma segura con los recursos de su empresa que están protegidos por el firewall. También admite BlackBerry Dynamics Direct Connect, que permite que los datos de aplicaciones omitan BlackBerry Dynamics NOC. Para obtener más información, consulte Configuración de las propiedades y la comunicación de red para las aplicaciones BlackBerry Dynamics.
BlackBerry Secure Connect Plus	BlackBerry Secure Connect Plus proporciona a los usuarios acceso a los recursos de trabajo que se encuentran detrás del firewall de la empresa, a la vez que garantiza que los datos estén protegidos mediante protocolos estándar y cifrado integral. Para obtener más información, consulte Uso de BlackBerry Secure Connect Plus en las conexiones con los recursos de trabajo.
BlackBerry Secure Gateway	BlackBerry Secure Gateway proporciona a los dispositivos iOS que utilizan el tipo de activación Controles de MDM una conexión segura con el servidor de correo de la empresa a través de BlackBerry Infrastructure. Para más información, consulte Protección de los datos de correo electrónico enviados a dispositivos iOS mediante BlackBerry Secure Gateway.

Componente	Finalidad
BlackBerry Gatekeeping Service	BlackBerry Gatekeeping Service facilita el control de los dispositivos que pueden acceder a Exchange ActiveSync. Para obtener más información, consulte Supervisión de los dispositivos que pueden acceder a Exchange ActiveSync.

Los archivos de instalación y de activación de BlackBerry Connectivity Node están disponibles en la consola de administración UEM. Puede utilizar estos archivos para instalar nuevas instancias de BlackBerry Connectivity Node y para actualizar las instancias existentes.

Pasos para instalar y activar BlackBerry Connectivity Node

Puede instalar una o más instancias de BlackBerry Connectivity Node para mejorar la redundancia.

Paso	Acción
1	Revise los requisitos y consideraciones para instalar BlackBerry Connectivity Node.
2	Instalar y configurar BlackBerry Connectivity Node.
3	De forma opcional, Creación de un grupo de servidores para administrar las conexiones regionales.
4	Realizar una configuración adicional para las aplicaciones BlackBerry Secure Connect Plus, BlackBerry Secure Gateway, BlackBerry Gatekeeping Service y BlackBerry Dynamics.

Requisitos: BlackBerry Connectivity Node

Elemento	Requisitos o consideraciones
Hardware	Instale el BlackBerry Connectivity Node en un equipo específico reservado para fines técnicos, no en un equipo que se utilice para el trabajo diario. El ordenador debe tener acceso a Internet y al directorio de la empresa. No puede instalar BlackBerry Connectivity Node en un ordenador que ya aloja una instancia de BlackBerry UEM local. Puede instalar una o más instancias de BlackBerry Connectivity Node para mejorar la redundancia. Debe instalar cada instancia en un ordenador específico. Cualquier equipo que aloje BlackBerry Connectivity Node debe cumplir los siguientes requisitos: • 6 núcleos de procesador, E5-2670 (2,6 GHz), E5-2683 v4 (2,1 GHz) o equivalente • 12 GB de memoria disponible • 64 GB de espacio en disco
Modo de rendimiento de servicio único	Opcionalmente, puede designar cada BlackBerry Connectivity Node de un grupo de servidores para administrar un único tipo de conexión: solo BlackBerry Secure Connect Plus, solo BlackBerry Secure Gateway o solo BlackBerry Proxy. Esto puede liberar recursos para admitir que haya menos servidores para el mismo número de usuarios o contenedores. Cada BlackBerry Connectivity Node habilitado para el modo de rendimiento de un solo servicio puede admitir hasta 10 000 dispositivos. Si activa el modo de rendimiento de servicio único para un BlackBerry Connectivity Node, tenga en cuenta los siguientes ajustes en los requisitos de hardware indicados anteriormente: • Solo BlackBerry Secure Connect Plus: 4 núcleos de procesador, E5-2670 (2,6 GHz), E5-2683 v4 (2,1 GHz) o equivalente • Solo BlackBerry Secure Gateway: 8 núcleos de procesador, E5-2670 (2,6 GHz), E5-2683 v4 (2,1 GHz) o equivalente • Solo BlackBerry Proxy: no hay diferencias.
Escalabilidad y alta disponibilidad	Cada BlackBerry Connectivity Node puede admitir hasta 5000 dispositivos. Puede instalar instancias adicionales para admitir hasta 50 000 dispositivos adicionales. Puede implementar más de un BlackBerry Connectivity Node en un grupo de servidores para permitir una alta disponibilidad y equilibrar la carga.

Elemento	Requisitos o consideraciones
Software	Cualquier equipo que aloje una instancia de BlackBerry Connectivity Node debe cumplir los siguientes requisitos: • Un SO compatible • Windows PowerShell 2.0 o posteriores; necesario para que la aplicación de configuración instale el servicio RRAS para BlackBerry Secure Connect Plus y BlackBerry Gatekeeping Service • Instale la versión necesaria del JRE y defina la variable BB_JAVA_HOME. Para obtener más información, consulte Establecer una variable de entorno para la ubicación de Java.
Conexiones del directorio	Compruebe que esté utilizando un servicio de directorio compatible. Puede configurar una o más conexiones de directorio, pero si tiene varias instancias BlackBerry Connectivity Node, todas las conexiones de directorio deben configurarse de forma idéntica. Si falta una conexión de directorio o está configurada incorrectamente, ese BlackBerry Connectivity Node aparecerá como desactivado en la consola de gestión.
Puertos	Verifique que los siguientes puertos salientes estén abiertos en el firewall de su empresa, de manera que los componentes de BlackBerry Connectivity Node (y sus correspondientes servidores proxy) puedan comunicarse con BlackBerry Infrastructure: • 443 (HTTPS) para activar BlackBerry Connectivity Node • 3101 (TCP) para las demás conexiones salientes
Cuentas de administrador	Al instalar y configurar BlackBerry Connectivity Node, utilice cuentas de administrador que cumplan los siguientes requisitos: • Utilice una cuenta de Windows con permisos para instalar y configurar software en el ordenador. • Elija una cuenta de directorio con permisos de lectura para cada conexión de directorio que desee configurar. • Utilice una cuenta de administrador de UEM Cloud con permisos para descargar los archivos de instalación y activación de BlackBerry Connectivity Node (por ejemplo, administrador de seguridad).

Instalar y configurar BlackBerry Connectivity Node

Antes de empezar:

- Revise los requisitos y consideraciones para instalar BlackBerry Connectivity Node.
- En la barra de menús de la consola de gestión, haga clic en **Configuración > Integración externa > Configuración de BlackBerry Connectivity Node**. Haga clic en y descargue la aplicación de configuración de BlackBerry Connectivity Node. Si desea agregar la instancia de BlackBerry Connectivity Node a un grupo de servidores existente cuando lo activa, en la lista desplegable **Grupo de servidores**, haga clic en el grupo de servidores correspondiente. Genere y guarde el archivo de activación. El archivo de activación será válido durante 60 minutos.

- Transfiera la aplicación de instalación y el archivo de activación al equipo en el que desea alojar la instancia BlackBerry Connectivity Node. Realice los pasos que se indican a continuación en ese equipo.

1. Ejecute la aplicación de configuración BlackBerry Connectivity Node.
2. Seleccione su idioma. Haga clic en **Aceptar**.
3. Haga clic en **Siguiente**.
4. Seleccione un país o una región. Lea y acepte el contrato de licencia. Haga clic en **Siguiente**.
5. El programa de instalación verifica que el equipo cumpla con los requisitos de instalación. Haga clic en **Siguiente**.
6. Para cambiar la ruta del archivo de instalación, haga clic en **...** y vaya a la ruta del archivo que desea utilizar. Haga clic en **Install (Instalar**).
7. Cuando finalice la instalación, haga clic en **Siguiente**.

   Se muestra la dirección de la consola de BlackBerry Connectivity Node (http:/localhost:8088). Haga clic en el enlace y guarde el sitio en su navegador.
8. Seleccione su idioma. Haga clic en **Siguiente**.
9. Cuando se activa BlackBerry Connectivity Node, envía los datos a través del puerto 443 (HTTPS) a BlackBerry Infrastructure (por ejemplo, na.bbsecure.com o eu.bbsecure.com). Después de activarlo, BlackBerry Connectivity Node utiliza el puerto 3101 (TCP) para todas las demás conexiones salientes a través de BlackBerry Infrastructure. Si desea enviar los datos de BlackBerry Connectivity Node a través de un servidor proxy existente situado detrás el firewall de la empresa, haga clic en **Haga clic aquí para configurar los ajustes de proxy para el entorno de su empresa**, seleccione la opción **Servidor proxy** y realice alguna de las siguientes acciones:
   - Para enviar datos de activación a través de un servidor proxy, en el campo **Proxy de inscripción**, escriba el FQDN o la dirección IP y el número de puerto del servidor proxy. El servidor proxy debe poder enviar datos a través del puerto 443 a .bbsecure.com. Haga clic en **Guardar**.
   - Para enviar otras conexiones salientes desde los componentes de BlackBerry Connectivity Node a través de un servidor proxy, en los campos correspondientes, escriba el FQDN o la dirección IP y el número de puerto del servidor proxy. El servidor proxy debe poder enviar datos a través del puerto 3101 a .bbsecure.com. Haga clic en **Guardar**.
10. En el campo **Nombre descriptivo**, escriba un nombre para BlackBerry Connectivity Node. Haga clic en **Siguiente**.
11. Haga clic en **Examinar**. Seleccione el archivo de activación.
12. Haga clic en **Activar**.

    Si desea añadir una instancia de BlackBerry Connectivity Node a un grupo de servidores existente durante la activación, el firewall de la empresa debe permitir las conexiones de ese servidor a través del puerto 443 mediante BlackBerry Infrastructure para activar BlackBerry Connectivity Node y a la misma región bbsecure.com como la instancia principal de BlackBerry Connectivity Node.
13. Haga clic en + y seleccione el tipo de directorio de empresa que desea configurar.
14. Siga los pasos para el tipo de directorio de la empresa:

Tipo de directorio	Pasos
Microsoft Active Directory	**a.** En el campo **Nombre de conexión**, escriba un nombre para la conexión de directorio. Si tiene configurado un directorio de Microsoft Entra ID, este nombre de conexión debe ser diferente del nombre de la conexión del directorio Entra. **b.** En el campo **Nombre de usuario**, escriba el nombre de usuario de la cuenta de Microsoft Active Directory. **c.** En el campo **Dominio**, escriba el FQDN del dominio que aloja Microsoft Active Directory. Por ejemplo, dominio.ejemplo.com. **d.** En el campo **Contraseña**, escriba la contraseña de la cuenta de Microsoft Active Directory. **e.** En la lista desplegable **Detección del controlador de dominio**, haga clic en una de las acciones siguientes: • Si desea utilizar la detección automática, haga clic en **Automático**. • Si desea especificar el ordenador del controlador de dominio, haga clic en **Seleccionar de la lista a continuación**. Haga clic en + y escriba el FQDN del equipo. Repita este paso para agregar más ordenadores. **f.** En el campo **Base de búsqueda del catálogo global**, escriba la base de búsqueda a la que desea acceder (por ejemplo, OU=Users,DC=example,DC=com). Para buscar en todo el catálogo global, deje el campo en blanco. **g.** En la lista desplegable **Detección de catálogo global**, haga clic en una de las acciones siguientes: • Si desea utilizar la detección de catálogo automática, haga clic en **Automático**. • Si desea especificar el ordenador del catálogo, haga clic en **Seleccionar de la lista a continuación.** Haga clic en + y escriba el FQDN del equipo. Si es necesario, repita este paso para especificar más ordenadores. **h.** Si desea activar la compatibilidad con los buzones 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 UEM Cloud acceda, en la sección **Lista de bosques de cuentas**, haga clic en +. Especifique el nombre del bosque y el nombre del dominio de usuario (el usuario puede pertenecer a cualquier dominio del bosque de cuentas), así como el nombre de usuario y la contraseña. **i.** 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. **j.** Haga clic en **Guardar**.

Tipo de directorio	Pasos
Directorio de LDAP	**a.** En el campo **Nombre de conexión**, escriba un nombre para la conexión de directorio. Si tiene configurado un directorio de Microsoft Entra ID, este nombre de conexión debe ser diferente del nombre de la conexión del directorio Entra. **b.** En la lista desplegable **Detección del servidor LDAP**, haga clic en una de las siguientes opciones: • Si desea utilizar la detección automática, haga clic en **Automático**. En el campo **Nombre del dominio DNS**, escriba el nombre del dominio DNS. • Si desea especificar el ordenador de LDAP, haga clic en **Seleccionar servidor de la lista a continuación**. Haga clic en + y escriba el FQDN del equipo. Repita este paso para agregar más ordenadores. **c.** En la lista desplegable **Activar SSL**, seleccione si desea activar la autenticación SSL para el tráfico LDAP. Si hace clic en **Sí**, haga clic en **Explorar** y seleccione el certificado SSL para el ordenador LDAP. **d.** En el campo del puerto **LDAP**, escriba el número de puerto del ordenador de LDAP. **e.** En la lista desplegable **Autorización requerida**, seleccione si UEM Cloud debe autenticarse con el equipo LDAP. Si hace clic en **Sí**, introduzca el nombre de usuario y la contraseña de la cuenta de LDAP. El nombre de usuario debe escribirse en formato DN (por ejemplo, CN=Megan Ball,OU=Sales,DC=example,DC=com). **f.** En el campo **Base de búsqueda**, introduzca la base de búsqueda a la que desea acceder (por ejemplo, OU=Users,DC=example,DC=com). **g.** En el campo **Filtro de búsqueda LDAP de usuario**, introduzca el filtro que desea utilizar para los usuarios de LDAP. Por ejemplo: (&(objectCategory=person)(objectclass=user)(memberOf=CN=Local,OU=Users,DC=example,DC=com)). **h.** En la lista desplegable **Ámbito de búsqueda de usuario de LDAP**, haga clic en una de las siguientes opciones: • Si desea que las búsquedas de usuario se apliquen a todos los niveles por debajo del DN de base, haga clic en **Todos los niveles**. • Si desea limitar las búsquedas de usuario a un nivel por debajo del DN de base, haga clic en **Un nivel**. **i.** En el campo **Identificador único**, introduzca el atributo del identificador único de cada usuario (por ejemplo, uid). Este atributo debe ser invariable y exclusivo globalmente de cada usuario. **j.** En el campo **Nombre**, introduzca el atributo del nombre de cada usuario (por ejemplo, givenName). **k.** En el campo **Apellido**, introduzca el atributo del apellido de cada usuario (por ejemplo, sn). **l.** En el campo **Atributo de inicio de sesión**, introduzca el atributo del atributo de inicio de sesión de cada usuario (por ejemplo, cn). Este atributo se utiliza para el valor que los usuarios escriben para iniciar sesión en BlackBerry UEM Self-Service con sus credenciales de directorio. **m.** En el campo **Dirección de correo**, escriba el atributo del correo de cada usuario (por ejemplo, correo). **n.** En el campo **Nombre para mostrar**, introduzca el atributo del nombre para mostrar de cada usuario (por ejemplo, displayName). **o.** 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. **p.** Para permitir los grupos vinculados a directorios, seleccione la casilla de verificación **Permitir los grupos vinculados a directorios**. Para obtener más información sobre los grupos vinculados a directorios, consulte Permitir los grupos vinculados al directorio.

15. En la consola de gestión, haga clic en **Configuración > Integración externa > Configuración de BlackBerry Connectivity Node**.
16. En la sección **Paso 4: Probar conexión**, haga clic en **Siguiente**.

Para ver el estado de una instancia de BlackBerry Connectivity Node, en la barra de menú de la consola de gestión, haga clic en **Configuración > Integración externa > Estado de BlackBerry Connectivity Node**.

Después de terminar:

- Para instalar instancias adicionales de BlackBerry Connectivity Node, vuelva a descargar los archivos de instalación y activación y repita esta tarea en un equipo diferente. Esta operación debe efectuarse tras activar la primera instancia.
- Si instala más de una BlackBerry Connectivity Node, debe configurar conexiones de directorio idénticas en cada instancia. Puede utilizar la consola BlackBerry Connectivity Node para exportar las conexiones de directorio de una instancia (archivo .txt) y, después, transferir e importar esas conexiones a un BlackBerry Connectivity Node diferente con la consola de esa instancia. Elimine cualquier conexión de directorio existente de una instancia antes de importar configuraciones de directorio.
- De forma opcional, Creación de un grupo de servidores para administrar las conexiones regionales.
- Si desea enviar datos a través de un proxy HTTP antes de que llegue a BlackBerry Dynamics NOC, en la consola de BlackBerry Connectivity Node, haga clic en **Configuración general > Router y proxy de BlackBerry**. Seleccione la casilla de verificación **Activar proxy HTTP** y configure los ajustes del proxy.
- Si desea cambiar la configuración predeterminada para las instancias de BlackBerry Connectivity Node, en la barra de menús de la consola de administración, haga clic en **Configuración > Integración externa> Configuración de BlackBerry Connectivity Node** y haga clic en . Puede cambiar la configuración de registro, deshabilitar instancias de BlackBerry Gatekeeping Service y configurar los ajustes de BlackBerry Secure Gateway.
- Cuando reciba una notificación de una actualización de BlackBerry Connectivity Node, repita esta tarea para actualizar cada instancia. Utilice la consola BlackBerry Connectivity Node para registrar o exportar configuraciones de directorio. Debe actualizar todas las instancias de BlackBerry Connectivity Node a la misma versión. Al actualizar la primera instancia, los servicios de directorio se desactivan hasta que todos los nodos se actualicen a la misma versión.
- Para obtener instrucciones para activar BlackBerry Secure Connect Plus, consulte Uso de BlackBerry Secure Connect Plus en las conexiones con los recursos de trabajo en el contenido de Administración.
- Para obtener instrucciones sobre la activación de BlackBerry Secure Gateway, consulte Protección de los datos de correo electrónico enviados a dispositivos iOS mediante BlackBerry Secure Gateway en el contenido de Administración.
- Para obtener instrucciones sobre la configuración de BlackBerry Gatekeeping Service, consulte Control de los dispositivos que pueden acceder a Exchange ActiveSync en el contenido de Administración.

Creación de un grupo de servidores para administrar las conexiones regionales

Si desea administrar conexiones regionales para las características de conectividad de empresa que ofrece BlackBerry Connectivity Node, puede implementar varias instancias de BlackBerry Connectivity Node en una región dedicada como un grupo de servidores. Al crear un grupo de servidores, debe especificar la ruta de datos regionales que desea que los componentes usen para conectarse a BlackBerry Infrastructure. Los grupos de servidores también admiten redundancia, alta disponibilidad y equilibrio de carga para las instancias BlackBerry Connectivity Node.

Antes de empezar: Instalar y configurar varias instancias de BlackBerry Connectivity Node.

1. En la barra de menús de la consola de gestión, haga clic en **Configuración > Integración externa > Configuración de BlackBerry Connectivity Node**.
2. Haga clic en .
3. Escriba un nombre y una descripción para el grupo de servidores.
4. En la lista desplegable **País**, seleccione el país correspondiente.
5. Si desea desactivar la conexión del directorio de empresa para las instancias en el grupo de servidores, seleccione la casilla de verificación **Anular configuración de Directory Service**.
6. De forma predeterminada, BlackBerry Gatekeeping Service se activa en cada instancia de BlackBerry Connectivity Node. Si desea que los datos de enlace solo los gestione la instancia principal de BlackBerry Connectivity Node, seleccione la casilla para marcar **Anular configuración de BlackBerry Gatekeeping Service** para desactivar cada BlackBerry Gatekeeping Service en el grupo de servidores.
7. Si desea utilizar una configuración de DNS para BlackBerry Secure Connect Plus que sea diferente a la configuración predeterminada (**Configuración > Infraestructura > BlackBerry Secure Connect Plus**), seleccione la casilla de verificación **Anular servidores DNS**. Siga estas instrucciones:
   a) En la sección **Servidores DNS**, haga clic en +. Escriba la dirección del servidor DNS con notación decimal con puntos (por ejemplo, 192.0.2.0). Haga clic en **Agregar**. Repita según sea necesario.
   b) En la sección **Sufijo de búsqueda DNS**, haga clic en +. Escriba el sufijo de búsqueda de DNS (por ejemplo, domain.com). Haga clic en **Agregar**. Repita según sea necesario.
8. Si desea configurar los ajustes de registro para las instancias de BlackBerry Connectivity Node en el grupo de servidores, seleccione la casilla de verificación **Anular configuración de registro**. Efectúe una de las acciones siguientes:
   - En la lista desplegable **Niveles de depuración del registro del servidor**, seleccione el nivel de registro adecuado.
   - Si desea enrutar los eventos de registro a un servidor syslog, seleccione la casilla de verificación **Syslog** y especifique el puerto y nombre de host del servidor syslog.
   - Si desea cambiar la configuración del registro local, seleccione la casilla de verificación **Activar destino de archivo local**. Especifique el límite de tamaño (en MB), el límite de antigüedad (en días) y seleccione si desea comprimir las carpetas de registro.
   - Si desea configurar diferentes niveles de registro para los componentes BlackBerry Connectivity Node, en la sección **Anulación de registro de servicio**, haga clic en + y seleccione el componente y el nivel de registro adecuados. Repita según sea necesario.
9. Si desea usar las instancias del grupo de servidor para un solo tipo de conexión, seleccione la casilla de verificación **Activar modo de rendimiento de servicio único**. En el menú desplegable **Tipo de conexión**, seleccione el tipo de conexión (solo BlackBerry Secure Connect Plus, solo BlackBerry Secure Gateway o solo BlackBerry Proxy).
10. Si desea configurar los ajustes de BlackBerry Secure Gateway para las instancias del grupo de servidores, seleccione la casilla de verificación **Anular configuración de BlackBerry Secure Gateway**. Para dispositivos iOS que usen autenticación moderna para conectarse a Microsoft Exchange Online, especifique el recurso de servidor de correo y el extremo de detección:
    a) Seleccione la casilla de verificación **Activar OAuth para la autenticación del servidor de correo**.
    b) En el campo **Extremo de detección**, especifique la URL utilizada para las solicitudes de detección. Introduzca el extremo de detección en el formato https://<*identity provider*>/.well-known/openid-configuration (por ejemplo, `https://login.microsoftonline.com/common/.well-known/openid-configuration`) o `https://login.windows.net/common/.well-known/openid-configuration`).
    c) En el campo **Recurso del servidor de correo**, especifique la dirección URL del recurso del servidor de correo que se va a utilizar para las solicitudes de autorización y token mediante OAuth. Por ejemplo, `https://outlook.office365.com`.

11. Haga clic en **Guardar**.

Después de terminar: Seleccione el grupo de servidores y haga clic en para añadirle las instancias BlackBerry Connectivity Node. Puede añadir una instancia a un grupo de servidores o eliminar una instancia de un grupo de servidores en cualquier momento.

Resolución de problemas: BlackBerry Connectivity Node

Problema	Solución posible
BlackBerry Connectivity Node no se activa con UEM Cloud.	• Verifique que ha cargado el archivo de activación más reciente que haya generado en la consola de gestión. Solo es válido el último archivo de activación. • El archivo de activación caduca después de 60 minutos. Genere y cargue un nuevo archivo de activación y, a continuación, intente realizar de nuevo la activación. • Consulte KB 38964.

BlackBerry Connectivity Node no establece la conexión con UEM Cloud.	• Verifique que los siguientes puertos salientes estén abiertos en el firewall de la empresa, de manera que los componentes de BlackBerry Connectivity Node (y sus correspondientes servidores proxy) puedan comunicarse con BlackBerry Infrastructure (*region*.bbsecure.com):
	  • 443 (HTTPS) para activar BlackBerry Connectivity Node
	  • 3101 (TCP) para las demás conexiones salientes
	• Revise el archivo de registro más reciente para obtener información sobre el motivo por el que BlackBerry Connectivity Node no puede establecer conexión con UEM Cloud. De forma predeterminada, los archivos de registro se ubican en *<drive:>*:\Program Files\BlackBerry\BlackBerry Connectivity Node\Logs.

Problema	Solución posible
BlackBerry Connectivity Node no establece la conexión con el directorio de la empresa.	• Si tiene varias instancias de BlackBerry Connectivity Node, compruebe que todas tengan la misma versión. • Compruebe que ha especificado la configuración correcta para el directorio de la empresa. • Compruebe que todas las instancias tengan una conexión de directorio y que las conexiones de directorio estén configuradas de forma idéntica en todas las instancias. • Verifique que ha especificado la información de inicio de sesión correcta para la cuenta de directorio y que la cuenta dispone de los permisos necesarios para acceder al directorio de la empresa. • Compruebe que estén abiertos los puertos adecuados en el firewall de la organización. • Compruebe que no haya utilizado el mismo archivo de activación para dos instalaciones diferentes. • Compruebe que está utilizando el archivo de activación más reciente. • Revise el archivo de registro más reciente para obtener información sobre el motivo por el que BlackBerry Connectivity Node no puede acceder al directorio de la empresa. De forma predeterminada, los archivos de registro se ubican en *<drive:>*:\Program Files\BlackBerry \BlackBerry Connectivity Node\Logs. • Si utiliza Microsoft Active Directory, consulte KB 36955.

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

Puede utilizar las siguientes configuraciones de proxy en su entorno BlackBerry UEM:

Entorno	Opciones de proxy
UEM local	Puede configurar UEM para enviar datos a través de un servidor proxy antes de que lleguen a BlackBerry Infrastructure. De forma predeterminada, 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 un servidor proxy TCP. El servidor proxy TCP actúa como un intermediario entre UEM y BlackBerry Infrastructure. Puede instalar un servidor proxy fuera del firewall de la empresa en una DMZ. La instalación de un servidor proxy TCP en una DMZ proporciona un nivel adicional de seguridad para UEM. Solo el servidor proxy se conecta a UEM desde fuera del firewall. Todas las conexiones con BlackBerry Infrastructure entre UEM y los dispositivos se realizan a través del servidor proxy.
UEM Cloud	Para utilizar un servidor proxy con BlackBerry Connectivity Node, puede instalar BlackBerry Router para que actúe como un servidor proxy, o bien utilizar un servidor proxy TCP ya instalado en el entorno de su empresa. 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. Solo BlackBerry Router o el servidor proxy se conectan a BlackBerry Connectivity Node desde fuera del firewall. Todas las conexiones con BlackBerry Infrastructure entre BlackBerry Connectivity Node y los dispositivos se realizan a través del servidor proxy. De forma predeterminada, BlackBerry Connectivity Node 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 Connectivity Node y BlackBerry Infrastructure.

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

En entornos de UEM locales, puede configurar un servidor proxy TCP transparente para el servicio de BlackBerry UEM Core. 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.

En entornos UEM Cloud, BlackBerry Connectivity Node envía datos de activación a través del puerto 443 (HTTPS). Tras su activación, BlackBerry Connectivity Node envía y recibe datos a través del puerto 3101 (TCP). Se puede configurar BlackBerry Connectivity Node para enrutar datos HTTPS o TCP a través de un servidor proxy detrás del firewall de la empresa. BlackBerry Connectivity Node no admite la autenticación con un servidor proxy.

Se pueden configurar varios servidores proxy TCP configurados con SOCKS v5 (sin autenticación) para conectarse a 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.

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 UEM.

1. Siga los pasos para su entorno:

Entorno	Pasos
UEM local	**a.** En la barra de menús de la consola de administración, haga clic en **Configuración > Infraestructura > Enrutador y proxy BlackBerry**. **b.** En **Configuración global**, seleccione **Servidor proxy**. **c.** Por cada servicio para el que desee utilizar el servidor proxy, especifique el FQDN o la dirección IP y el número de puerto del servidor proxy. Cada campo requiere un valor único.
UEM Cloud	**a.** En la consola de BlackBerry Connectivity Node (http:/localhost:8088), haga clic en **Configuración general > Proxy**. **b.** Seleccione **Servidor proxy**. **c.** Si desea enrutar los datos de activación HTTPS para BlackBerry Connectivity Node a través de un servidor proxy, en los campos **Proxy de inscripción**, escriba el FQDN o la dirección IP y el número de puerto del servidor proxy. El servidor proxy debe poder enviar datos a través del puerto 443 a *<region>*.bbsecure.com. **d.** Si desea enrutar otras conexiones salientes desde los componentes de BlackBerry Connectivity Node a través de un servidor proxy, en los campos correspondientes, escriba el FQDN o la dirección IP y el número de puerto del servidor proxy. El servidor proxy debe poder enviar datos a través del puerto 3101 a *<region>*.bbsecure.com.

2. 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 UEM.

1. Lleve a cabo una de estas acciones:
   - En un entorno local de UEM, haga clic en **Configuración > Infraestructura > BlackBerry Router y proxy** en la barra de menús de la consola de administración.
   - En un entorno UEM Cloud, en la consola BlackBerry Connectivity Node (http:/localhost:8088), haga clic en **Configuración general > Proxy**.
2. Seleccione **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 nombre de host del servidor proxy SOCKS v5.

6. Haga clic en **Agregar**.
7. Repita los pasos del 2 al 6 para cada servidor proxy SOCKS v5 que quiera configurar.
8. En el campo **Puerto**, escriba el número de puerto.
9. Haga clic en **Guardar**.

Instalación de un BlackBerry Router independiente en un entorno UEM Cloud

BlackBerry Router es un componente opcional que se puede instalar en una DMZ fuera del firewall de la empresa. BlackBerry Router se conecta a Internet para enviar los datos entre BlackBerry Connectivity Node y los dispositivos que utilizan BlackBerry Infrastructure. BlackBerry Router funciona como un servidor proxy y puede ser compatible con SOCKS v5 (sin autenticación).

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. De forma predeterminada, BlackBerry Connectivity Node se conecta a BlackBerry Router mediante el puerto 3102. BlackBerry Router es compatible con todo el tráfico de salida de los componentes de BlackBerry Connectivity Node.

Antes de empezar:

- Debe instalar un BlackBerry Router independiente en un equipo que no aloje una instancia de BlackBerry Connectivity Node.
- Compruebe que dispone del nombre del host de SRP. El nombre de host de SRP es normalmente `<country code>.srp.blackberry.com` (por ejemplo, `us.srp.blackberry.com`).

1. En la barra de menú de la consola de gestión de UEM, haga clic en **Configuración > Integración externa > Configuración de BlackBerry Connectivity Node**.
2. Haga clic en .
3. Haga clic en **Descargar**.
4. En la página de descarga del software, responda a las preguntas necesarias y haga clic en **Descargar**. Guarde y extraiga el paquete de instalación.
5. En la carpeta **enrutador**, extraiga el archivo ZIP **setupinstaller**. Este archivo ZIP contiene una carpeta **Instalador** que dispone de un archivo **Setup.exe** que puede utilizar para instalar BlackBerry Router.
6. Transfiera el archivo **Setup.exe** al equipo en el que desea instalar BlackBerry Router y haga doble clic en él para ejecutar la aplicación de instalación.

   La instalación se ejecuta en segundo plano y no muestra cuadros de diálogo. Una vez finalizada la instalación, el servicio BlackBerry Router aparece en la ventana de servicios.
7. En la consola de BlackBerry Connectivity Node (http:/localhost:8088), haga clic en **Configuración general > Proxy**.
8. Seleccione **Router de BlackBerry**.
9. Haga clic en +.
10. Escriba la dirección IP o el nombre de host de la instancia de BlackBerry Router que desee conectar a UEM.
11. Haga clic en **Agregar**.
12. En el campo **Puerto**, escriba el número de puerto que todas las instancias de BlackBerry Router escuchan. El valor predeterminado es 3102.
13. 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, puede que necesite configurar su entorno BlackBerry UEM local para:

- Permitir que el UEM Core se comunique con la consola de administración si está instalada en otro equipo.
- Permitir que el UEM se comunique con otros servicios internos, como entidades de certificación y servidores que alojan aplicaciones de inserción.

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

1. En la barra de menús de la consola de administración, haga clic en **Configuración > Infraestructura > Proxy del lado del servidor**.
2. Lleve a cabo una de estas acciones:

Tarea	Pasos
Configure los valores de proxy globales para la mayoría o todos los servidores del dominio UEM.	**a.** Amplíe **Configuración de proxy global del lado del servidor**. **b.** En la lista desplegable **Tipo**, haga clic en **Configuración PAC** o **Configuración manual**. **c.** Complete los campos obligatorios. **d.** Haga clic en **Guardar**.
Configure los valores de proxy para uno o más servidores que sean diferentes de los valores de proxy globales.	**a.** Amplíe nombre del servidor. **b.** En la lista desplegable **Tipo**, haga clic en **Ninguno**, **Configuración PAC** o **Configuración manual**. **c.** Complete los campos obligatorios. **d.** Haga clic en **Guardar**.

Conexión a un servidor SMTP para enviar notificaciones de correo

Debe conectar BlackBerry UEM local a un servidor SMTP para que pueda enviar instrucciones de activación, advertencias de conformidad del dispositivo, contraseñas para UEM Self-Service y notificaciones de correo electrónico a los usuarios de dispositivos.

1. En la barra de menús de la consola de administración, 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 electrónico de UEM (por ejemplo, `donotreply` o `UEM Admin`.
4. En el campo **Dirección del remitente**, escriba la dirección de correo electrónico que desea que UEM utilice para enviar notificaciones por correo.
5. En el campo **Servidor SMTP**, escriba el FQDN del servidor SMTP.
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 la lista desplegable **Tipo de cifrado compatible**, seleccione el tipo de cifrado adecuado.
8. Si el servidor SMTP requiere autenticación, especifique el nombre de usuario y la contraseña.
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, selecciónelo 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. UEM envía el mensaje a la dirección de correo electrónico especificada en el campo **Dirección del remitente**.

Conexión con los directorios de la empresa

Puede conectar BlackBerry UEM al directorio de empresa de su organización para aprovechar las siguientes funciones:

- Puede crear cuentas de usuario en UEM mediante el uso de datos del usuario del directorio y UEM puede autenticar a los administradores para la consola de gestión y los usuarios para BlackBerry UEM Self-Service.
- Puede vincular grupos de directorios de la empresa con grupos UEM para organizar a los usuarios de la misma forma que se organizan en el directorio de la empresa, y para simplificar la asignación y la gestión de las políticas de TI, los perfiles y las aplicaciones para los usuarios. Estos se denominan grupos vinculados a directorios.
- Puede activar la integración para grupos específicos en el directorio de la empresa para crear usuarios de UEM automáticamente. Estos se denominan grupos de directorio de integración. Al añadir nuevos usuarios a estos grupos de directorios, se crean nuevas cuentas de usuario para dichos usuarios en UEM. Si activa la integración, también puede configurar la extracción para eliminar datos de dispositivos o cuentas de usuario de UEM cuando los usuarios se desactivan o eliminan del directorio de su empresa.

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

Paso	Acción
1	En un entorno UEM local, Conexión a una instancia de Microsoft Active Directory o Conexión a un directorio LDAP. En un entorno UEM Cloud, instale y configure BlackBerry Connectivity Node para conectarse al directorio de la empresa. Para obtener instrucciones sobre la conexión UEM local o UEM Cloud a Entra ID, consulte Conexión de BlackBerry UEM a Microsoft Entra ID.
2	De forma opcional, Permitir los grupos vinculados al directorio.
3	De forma opcional, Activación y configuración de la integración y la extracción.
4	De forma opcional, configure la sincronización de directorios.

Conexión a una instancia de Microsoft Active Directory

La tarea de abajo se aplica a un entorno UEM local. En un entorno UEM Cloud, instale y configure BlackBerry Connectivity Node para conectarse al directorio de la empresa.

Antes de empezar:

- Cree una cuenta de Microsoft Active Directory que 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.

- Si su organización utiliza un bosque de recursos Microsoft Exchange, debe crear un buzón en el bosque de recursos para cada cuenta de usuario y asociarlos a las cuentas de usuario en los bosques de cuentas. UEM utiliza los buzones de correo para buscar las cuentas de usuario en los distintos dominios. Para autenticar los usuarios que inician sesión en UEM o 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 UEM que se encuentre en un dominio Windows que forme parte del bosque de recursos. Al crear la conexión de directorio, proporcione las credenciales de Windows para la cuenta Microsoft Active Directory y, en caso de que sea necesario, los nombres de los servidores de catálogo global que UEM puede utilizar.

1. En la barra de menús de la consola de administración de UEM, haga clic en **Configuración > Integración externa > Directorio de empresa**.
2. Haga clic en + **> 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**, haga una de las siguientes acciones:
   - Para permitir que UEM detecte automáticamente los centros de distribución de claves (KDC), haga clic en **Automático**.
   - Para especificar la lista de KDC de 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 utilice UEM.
8. En la lista desplegable **Selección de catálogo global**, haga una de las acciones siguientes:
   - Si desea que UEM detecte automáticamente los servidores de catálogo global, haga clic en **Automático**.
   - Para especificar la lista de servidores de catálogo global que 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 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**, haga una de las siguientes acciones:
    - Para permitir a UEM buscar en el catálogo global, deje el campo en blanco.
    - Para controlar qué cuentas de usuario pueden autenticar 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**, haga clic en el dominio que desea añadir. La selección predeterminada para el campo **¿Especificar nombre de usuario y contraseña?** es No. Si mantiene esta selección predeterminada, se utilizarán el nombre de usuario y la contraseña para la conexión del bosque. Si selecciona Sí, debe proporcionar unas credenciales válidas para una cuenta de Active Directory en el dominio que haya seleccionado. En el campo **Selección de KDC**, puede seleccionar Automático para permitir que UEM descubra automáticamente los centros de distribución de claves o Manual para especificar la lista de KDC que UEM utilizará para la autenticación. Haga clic en **Agregar**.

12. Si su entorno tiene un bosque de recursos deMicrosoft Exchange, para activar la compatibilidad con los buzones de correo de Microsoft Exchange vinculados, en la lista desplegable **Compatibilidad con buzones de correo vinculados de Microsoft Exchange**, haga clic en **Sí**.

    Para configurar la cuenta de Microsoft Active Directory para cada bosque al que desea que 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 UEM busque. Si es necesario, especifique los servidores de catálogo global a los que desea que 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 acerca del inicio de sesión único, consulte Configurar el inicio de sesión único para BlackBerry UEM en el contenido de Administración.
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:

- Haga cualquiera de las siguientes tareas opcionales:
  - Permitir los grupos vinculados al directorio.
  - Activación y configuración de la integración y la extracción.
  - Configurar sincronización de directorio.
- Si elimina una conexión a un directorio, todos los usuarios que se añadieron a UEM desde ese directorio 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 desde el directorio de la empresa.

Conexión a un directorio LDAP

La tarea de abajo se aplica a un entorno UEM local. En un entorno UEM Cloud, instale y configure BlackBerry Connectivity Node para conectarse al directorio de la empresa.

Antes de empezar:

- Cree una cuenta LDAP de UEM que se ubique en el directorio LDAP pertinente. La cuenta debe cumplir los siguientes requisitos:
  - La cuenta debe tener permiso para leer todos los usuarios del directorio.
  - La contraseña debe configurarse para que no caduque y no necesita cambiarse 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 de que el servidor LDAP admita TLS 1.2. Si se ha activado SSL, la conexión LDAP con UEM debe usar TLS 1.2.
- Verifique los valores de atributo LDAP que utiliza su empresa (los pasos siguientes proporcionan ejemplos de valores de atributo típicos); los utilizará en los pasos siguientes.

1. En la barra de menús de la consola de administración de UEM, haga clic en **Configuración > Integración externa > Directorio de empresa**.
2. Haga clic en + **> 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**, realice una de las siguientes acciones:
   - 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 añadir 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**, realice 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)`.
10. En la lista desplegable **Ámbito de búsqueda de usuario de LDAP**, realice 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`.
12. En el campo **Nombre**, escriba el atributo del nombre de cada usuario (por ejemplo, `givenName`).
13. En el campo **Apellidos**, escriba el atributo de los apellidos 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**, escriba 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 principal del usuario**, escriba el nombre principal del usuario para SCEP (por ejemplo, `mail`).
18. En el campo **Departamento**, escriba el atributo del departamento de cada usuario.
19. En el campo **Cargo**, escriba el atributo del cargo de cada usuario.
20. Si desea sincronizar campos adicionales del directorio LDAP, seleccione la casilla de verificación **Sincronizar detalles adicionales del usuario**. Escriba los atributos de los campos adicionales según sea necesario.
21. Para activar los grupos vinculados a directorios en la conexión de directorio, seleccione la casilla de verificación **Permitir los grupos vinculados a directorios**.
    a) 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.
    b) 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)`.
    c) 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`).
    d) En el campo **Nombre para mostrar del grupo**, escriba el atributo de nombre para mostrar de cada grupo (por ejemplo `cn`).
    e) En el campo **Atributo de pertenencia al grupo**, escriba el nombre del atributo de pertenencia al grupo. Los valores del atributo deben estar en formato DN (por ejemplo, `CN=jsmith,CN=Users,DC=example,DC=com`).
    f) En el campo **Probar nombre de grupo**, escriba el nombre de un grupo actual para validar los atributos de grupo especificados.
    g) Si desea habilitar la búsqueda paginada para los miembros del grupo, seleccione la casilla de verificación **Habilitar búsqueda de grupo paginada**.
22. Haga clic en **Guardar**.
23. Haga clic en **Cerrar**.

Después de terminar:

- Haga cualquiera de las siguientes tareas opcionales:
  - Permitir los grupos vinculados al directorio.
  - Activación y configuración de la integración y la extracción.
  - Configurar sincronización de directorio.
- Si elimina una conexión a un directorio, todos los usuarios que se añadieron a UEM desde ese directorio 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 desde el directorio de la empresa.

Permitir los grupos vinculados al directorio

Puede vincular grupos de BlackBerry UEM a grupos del directorio de su empresa para organizar a los usuarios de UEM de la misma forma que se organizan en el directorio y para simplificar la asignación y gestión de políticas de TI, perfiles y aplicaciones para los usuarios. Para obtener más información, consulte Creación y administración de grupos de usuarios en el contenido de Administración.

Antes de empezar:

- Conectar al directorio de su empresa:
  - UEM local: Conexión a una instancia de Microsoft Active Directory o Conexión a un directorio LDAP.

    - UEM Cloud: instalar y configurar BlackBerry Connectivity Node para conectarse a Microsoft AD o LDAP.
    - Local o en la nube: Conectar UEM a Microsoft Entra ID.
- 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 de la consola de administración, haga clic en **Configuración > Integración externa > Directorio de empresa**.
2. Haga clic en una conexión del directorio de la empresa.
3. En la pestaña **Sincronizar configuración**, seleccione la casilla de verificación **Permitir los grupos vinculados a directorios**.
4. Si desea forzar la sincronización de los grupos de directorios de la empresa, seleccione la casilla de verificación **Forzar sincronización**.

   Si se activa, cuando un grupo se elimina del directorio de su empresa, los vínculos a ese grupo se eliminan de los grupos vinculados a directorios y los 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.
5. En el campo **Límite de sincronización**, escriba el número máximo de cambios que puede completar cada proceso de sincronización.

   Si el número de cambios que deben sincronizarse supera el límite de sincronización, puede impedir que se ejecute el proceso de sincronización. UEM determina un total de los siguientes cambios: los usuarios que se añadirán 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:

- De forma opcional, Activación y configuración de la integración y la extracción.
- De forma opcional, configure la sincronización de directorios.
- Cree grupos vinculados a directorios. Para obtener más información, consulte Creación y administración de grupos de usuarios en el contenido de Administración.

Activación y configuración de la integración y la extracción

Al activar la integración, los grupos de directorios universales o globales se añaden a UEM como grupos de directorios de integración (la integración no es compatible con los grupos locales de dominio). Durante un proceso de sincronización, si UEM detecta un usuario de directorio en un grupo de directorios de integración que no tiene una cuenta de usuario UEM correspondiente, crea esa cuenta de usuario en UEM. Al habilitar la integración, también puede configurar la extracción; cuando se deshabilita o elimina un usuario de un grupo de directorios de integración, UEM puede eliminar los datos del dispositivo y eliminar al usuario de UEM.

Nota: Cuando se habilita la extracción, cualquier cuenta de usuario UEM que no sea miembro de un grupo de directorios de integración, independientemente de cómo se añadió a UEM, se extraerá durante el siguiente proceso de sincronización.

Antes de empezar:

- Conectar al directorio de su empresa:
    - UEM local: Conexión a una instancia de Microsoft Active Directory o Conexión a un directorio LDAP.
    - UEM Cloud: Instalar y configurar BlackBerry Connectivity Node para conectarse a Microsoft AD o LDAP.
    - Local o en la nube: Conectar UEM a Microsoft Entra ID.

- 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 de la consola de administración, haga clic en **Configuración > Integración externa > Directorio de empresa**.
2. Haga clic en una conexión del directorio de la empresa.
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. Efectúe una de las acciones siguientes:

Tarea	Pasos
Añada grupos de directorios de integración y configure las opciones de activación del dispositivo.	**a.** Haga clic en +. **b.** Busque y añada grupos de directorios universales o globales. **c.** Para cada grupo de directorios, seleccione si desea vincular grupos anidados. **d.** En la sección **Activación del dispositivo**, seleccione si desea que los usuarios integrados reciban una contraseña y una dirección de correo electrónico de activación generadas 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.
Integre los usuarios que solo desee que utilicen las aplicaciones BlackBerry Dynamics.	Siga estos pasos si desea integrar usuarios que solo utilizarán las aplicaciones BlackBerry Dynamics. Estos usuarios no activarán sus dispositivos en UEM mediante UEM Client, y UEM no administrará sus dispositivos. **a.** Seleccione la casilla de verificación **Integrar usuarios con las aplicaciones de BlackBerry Dynamics solamente**. **b.** Haga clic en +. **c.** Busque y añada grupos de directorios universales o globales. **d.** Para cada grupo de directorios, seleccione si desea vincular grupos anidados. **e.** Especifique el número de claves de acceso que se generarán por usuario, el periodo de caducidad de la clave de acceso y la plantilla de correo electrónico.

Tarea	Pasos
Configure la extracción.	Si desea eliminar los datos del dispositivo cuando se extrae un usuario de UEM, seleccione la casilla de verificación **Eliminar los datos del dispositivo cuando el usuario se haya eliminado de todos los grupos de directorio de integración**. Siga estas instrucciones: • Seleccione la opción adecuada para los datos que desea eliminar del dispositivo. • Si desea eliminar un usuario de UEM cuando se elimina de todos los grupos del directorio de integración, seleccione la casilla de verificación **Eliminar usuario cuando el usuario se haya eliminado de todos los grupos de directorio de integración**. • Si desea retrasar la eliminación de los usuarios y los datos del dispositivo durante dos horas después de un ciclo de sincronización, seleccione la casilla de verificación **Protección de la extracción**. Esta opción puede ayudar a evitar las eliminaciones inesperadas debido a la latencia de replicación de directorios.

6. Si desea forzar la sincronización de los grupos de directorios de la empresa, seleccione la casilla de verificación **Forzar sincronización**.

   Si se activa, cuando un grupo se elimina del directorio de su empresa, los vínculos a ese grupo se eliminan de los grupos vinculados a directorios y los 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.
7. En el campo **Límite de sincronización**, escriba el número máximo de cambios que puede completar cada proceso de sincronización.

   Si el número de cambios que deben sincronizarse supera el límite de sincronización, puede impedir que se ejecute el proceso de sincronización. UEM determina un total de los siguientes cambios: los usuarios que se añadirán 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.
8. En el campo **Nivel máximo de anidamiento de grupos de directorio**, escriba el número de niveles anidados para grupos de directorios de la empresa.
9. Haga clic en **Guardar**.

Después de terminar: De forma opcional, configure la sincronización de directorios.

Sincronización de una conexión de directorio

Después de conectar UEM al directorio de su empresa, puede iniciar manualmente el proceso de sincronización en cualquier momento o puede programar sincronizaciones periódicas. Puede obtener una vista previa de un informe de sincronización antes de que se produzca la siguiente sincronización y puede ver el informe después de que se complete un proceso de sincronización.

Antes de empezar:

- Conectar al directorio de su empresa:
  - UEM local: Conexión a una instancia de Microsoft Active Directory o Conexión a un directorio LDAP.
  - UEM Cloud: Instalar y configurar BlackBerry Connectivity Node para conectarse a Microsoft AD o LDAP.
  - Local o en la nube: Conectar UEM a Microsoft Entra ID.

- De forma opcional, Permitir los grupos vinculados al directorio y Activación y configuración de la integración y la extracción.

1. En la barra de menús de la consola de administración, haga clic en **Configuración > Integración externa > Directorio de empresa**.
2. Efectúe una de las acciones siguientes:

Tarea	Pasos
Vista previa de una sincronización.	**a.** Haga clic en para la conexión de directorio de la que desea obtener una vista previa de la sincronización. **b.** Haga clic en **Previsualizar ahora**. **c.** Cuando termine de procesar el informe, haga clic en la fecha en la columna **Último informe**.
Iniciar manualmente una sincronización de directorios.	**a.** Haga clic en para la conexión de directorio que desea sincronizar. **b.** Una vez finaliza la sincronización, haga clic en la fecha en la columna **Último informe**. **c.** Para exportar el informe en un archivo .csv, haga clic en .
Añadir un programa de sincronización.	**a.** Haga clic en la conexión de directorio para la que desea programar la sincronización. **b.** En la pestaña **Sincronizar programación**, haga clic en . **c.** En la lista desplegable **Tipo de sincronización**, seleccione una de las siguientes acciones: • **Todos los grupos y usuarios**: se integran y se retiran los usuarios según sea necesario, se sincronizan los cambios de pertenencia a grupos y se sincronizan los cambios en los atributos de usuario. • **Incorporación de grupos**: se incorporan y se retiran los usuarios según sea necesario y se sincronizan los cambios en los atributos de los usuarios. • **Grupos vinculados a directorios**: se sincronizan los cambios en la pertenencia a grupos y se sincronizan los cambios en los atributos de usuario. • **Atributos de usuario**: solo se sincronizan los cambios realizados en los atributos de usuario. **d.** En la lista desplegable **Repetición**, seleccione la opción adecuada y configure los ajustes de repetición según sea necesario. **e.** Haga clic en **Agregar**. **f.** Haga clic en **Guardar**.

Conexión de BlackBerry UEM a Microsoft Entra ID

Microsoft Entra ID es el servicio informático en la nube de Microsoft para la implementación y la gestión de aplicaciones y servicios. Conectar UEM a Entra proporciona las siguientes funciones:

- Puede conectar UEM con Entra ID para crear cuentas de usuario de directorio en UEM. Consulte Conexión de BlackBerry UEM a Entra ID.
- Puede utilizar UEM para crear, administrar y asignar perfiles de protección de aplicación Microsoft Intune para proteger los datos de las aplicaciones Office 365. Consulte Configuración de BlackBerry UEM para administrar perfiles de protección de aplicaciones Microsoft Intune.
- Si su empresa utiliza un acceso condicional Entra ID, puede configurar UEM como socio de cumplimiento para que Intune pueda reconocer el cumplimiento de los dispositivos gestionados por UEM al intentar acceder a sus aplicaciones basadas en la nube, como Office 365. Consulte Configuración de BlackBerry UEM como socio de cumplimiento de Intune en Entra.

Conexión de BlackBerry UEM a Entra ID

Puede conectar BlackBerry UEM a Microsoft Entra ID para crear cuentas de usuario de directorio en UEM. Después de configurar la conexión, puede buscar e importar datos de usuario desde el directorio para crear usuarios UEM. Los usuarios de directorio pueden utilizar las credenciales para acceder a BlackBerry UEM Self-Service. Si asigna un rol administrativo a un usuario de directorio, también podrá utilizar sus credenciales de directorio para iniciar sesión en la consola de administración.

Si su organización utiliza un Active Directory local y las cuentas están sincronizadas con Entra ID, debe crear una conexión de directorio para su Active Directory local (consulte Conexión a una instancia de Microsoft Active Directory). La conexión de UEM a Entra ID es adecuada cuando Entra ID es su servicio de directorio principal y no tiene un Active Directory local.

Antes de empezar: Debe tener una cuenta de Microsoft Entra ID. Si no tiene una cuenta, visite https://azure.microsoft.com para crear una cuenta. Utilice esa cuenta para iniciar sesión en el portal de Entra.

1. Inicie sesión en el portal Entra.
2. En la sección de registros de aplicaciones Entra ID, añada un nuevo registro.
3. Especifique lo siguiente y complete el registro:
   a) Escriba un nombre para el registro.
   b) Seleccione los tipos de cuenta que usarán la aplicación o accederán a la API.
   c) Para el URI de redirección, haga clic en **Web** y escriba `http://localhost`.
4. Copie el ID de aplicación.

   Este es el ID de cliente que registrará con UEM.
5. En la sección de administración de permisos de API (botón Registrar), añada un permiso y seleccione lo siguiente:
   - **Microsoft Graph**
   - **Permisos de aplicaciones**
   - Establezca los siguientes permisos: **Group.Read.All (Aplicación)**, **User.Read (Delegado)**, **User.Read.All (Aplicación)**
6. Conceda consentimiento de administrador a todas las cuentas del directorio actual.
7. En la sección de gestión de certificados y secretos, añada un nuevo secreto de cliente y especifique una descripción y duración.
8. Copie el campo de valor del nuevo secreto de cliente (no el ID del secreto).

Esta es la clave de cliente que registrará con UEM.

9. En la barra de menús de la consola de administración de UEM, haga clic en **Configuración > Integración externa > Directorio de empresa**.
10. Haga clic en + > **Conexión de Microsoft Azure Active Directory**.
11. En el campo **Nombre de la conexión de directorio**, escriba un nombre para la conexión.
12. En el campo **Dominio**, escriba el dominio de Entra ID.
13. En el campo **Id. de cliente**, introduzca el ID de cliente que ha registrado en el paso 4.
14. En el campo **Clave de cliente**, escriba el valor que ha registrado en el paso 8.
15. Haga clic en **Continuar**.
16. Haga clic en **Guardar**.

Después de terminar: Puede realizar cualquiera de las siguientes tareas opcionales:

- Permitir los grupos vinculados al directorio
- Activación y configuración de la integración y la extracción
- Sincronización de una conexión de directorio

Configuración de BlackBerry UEM para administrar perfiles de protección de aplicaciones Microsoft Intune

Si desea utilizar BlackBerry UEM para crear, gestionar y asignar perfiles de protección de aplicaciones Microsoft Intune para proteger los datos de las aplicaciones Office 365, debe hacer lo siguiente:

Paso	Acción
1	Revise la Requisitos previos para admitir la protección de la aplicación Intune.
2	Creación de un registro de aplicaciones en Entra.
3	Configurar BlackBerry UEM para que se sincronicen con Microsoft Intune.

Requisitos previos para admitir la protección de la aplicación Intune

- Para sincronizar BlackBerry UEM con Intune, debe utilizar una cuenta de administrador de Microsoft con una licencia Intune y con uno de los siguientes permisos en el portal Entra: administrador global, administrador limitado con el rol de administrador del servicio Intune o un rol personalizado con los permisos descritos en KB 50341.
- Las cuentas de usuario a las que desea asignar perfiles de protección de aplicaciones Intune deben existir en Entra ID.
- Los usuarios se deben añadir a UEM como usuarios del directorio.
- Si ha integrado su Microsoft Active Directory local, los usuarios deben sincronizarse con Entra ID. Para obtener más información, consulte la documentación de Microsoft de Entra ID Connect.

Creación de un registro de aplicaciones en Entra

Debe crear un registro de aplicaciones en Entra que UEM pueda utilizar para autenticarse con Entra.

Antes de empezar:

- Revise la Requisitos previos para admitir la protección de la aplicación Intune.
- En la barra de menús de la consola de administración de UEM, haga clic en **Configuración > Integración externa > Microsoft Intune**. Registre el valor de la **URL de respuesta**. Utilizará esta URL en el paso 3.

1. Inicie sesión en el portal Entra.
2. En la sección de registros de aplicaciones, añada un nuevo registro.
3. Especifique lo siguiente y complete el registro:
   a) Escriba un nombre para el registro.
   b) Seleccione los tipos de cuenta que usarán la aplicación o accederán a la API.
   c) Para URI de redirección, haga clic en **Cliente móvil/Escritorio** e introduzca la URL de respuesta desde la consola de administración.
4. Copie el ID de aplicación.

   Este es el ID de cliente que registrará con UEM.
5. En la sección de gestión de permisos de API, añada un permiso y seleccione lo siguiente:
   - **Microsoft Graph**
   - **Permisos delegados**
   - Configure los siguientes permisos delegados:
     - **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)**
6. Conceda consentimiento de administrador a todas las cuentas del directorio actual.
7. En la sección de gestión de certificados y secretos, añada un nuevo secreto de cliente y especifique una descripción y duración.
8. Copie el campo de valor del nuevo secreto de cliente (no el ID del secreto).

   Esta es la clave de cliente que registrará con UEM.

Después de terminar: Configurar BlackBerry UEM para que se sincronicen con Microsoft Intune.

Configurar BlackBerry UEM para que se sincronicen con Microsoft Intune

Antes de empezar: Creación de un registro de aplicaciones en Entra.

1. En la barra de menús de la consola de administración, haga clic en **Configuración > Integración externa > Microsoft Intune**.
2. En el campo **Id. de inquilino de Azure**, escriba el ID del inquilino Entra ID de su empresa.
3. En el campo **Id. de cliente**, introduzca el mismo ID de cliente que ha registrado en Creación de un registro de aplicaciones en Entra.
4. En el campo **Clave de cliente**, escriba el valor que ha registrado en Creación de un registro de aplicaciones en Entra.
5. Haga clic en **Siguiente**.
6. Especifique las credenciales de la cuenta de administrador de Intune que desea utilizar para el proceso de sincronización.

Después de terminar:

- Consulte Administración de aplicaciones protegidas por Microsoft Intune en el contenido de Administración.
- Si necesita volver a introducir las credenciales de la cuenta de administrador de Intune (por ejemplo, si se cambia la contraseña de la cuenta), vaya a **Configuración > Integración externa > Microsoft Intune** y haga clic en **Actualizar credenciales**.

Configuración de BlackBerry UEM como socio de cumplimiento de Intune en Entra

Si ha configurado el acceso condicional de Entra ID para su empresa, puede configurar BlackBerry UEM como socio de cumplimiento para que Intune pueda reconocer el cumplimiento de los dispositivos iOS y Android administrados por UEM al acceder a sus aplicaciones basadas en la nube, tales como Office 365. Puede configurar más de un inquilino UEM para cada inquilino Entra, pero todos los inquilinos UEM compartirán la misma entrada de gestión de socio de cumplimiento. Entra no puede diferenciar de qué inquilino UEM se origina una actualización de estado de cumplimiento.

Después de configurar UEM para el acceso condicional Entra ID, UEM informará a Entra ID cuando un dispositivo infrinja el cumplimiento.

Acción de aplicación del cumplimiento de UEM	Comportamiento
Acción de aplicación: supervisión y registro	No se informa de nada a Intune.
Acción de aplicación: • No confiar • Eliminar solo los datos de trabajo • Eliminar todos los datos	UEM informa a Entra ID cuando todos los mensajes de usuario han caducado.
Acción de aplicación para aplicaciones BlackBerry Dynamics: supervisión y registro	No se informa de nada a Intune.
Acción de aplicación para BlackBerry Dynamics: • No permitir la ejecución de aplicaciones de BlackBerry Dynamics • Eliminar datos de aplicaciones BlackBerry Dynamics	UEM informa a Entra ID tan pronto como se detecta la violación de conformidad.

Configuración de acceso condicional de Entra ID

Antes de empezar:

- Compruebe que tiene una cuenta Microsoft con una licencia Intune y con uno de los siguientes permisos en el portal Entra: administrador global, administrador limitado con el rol de administrador del servicio Intune o un rol personalizado con los permisos descritos en KB 50341.
- En el centro de administración de Microsoft Endpoint Manager, en la sección Gestión de conformidad de socios, añada **Acceso condicional de Azure de BlackBerry UEM** como socio de conformidad para los dispositivos iOS y Android y asígnelo a los usuarios y grupos.
- Para utilizar esta función, los usuarios del dispositivo deben cumplir con los requisitos siguientes:
  - Los usuarios deben existir en Entra ID y deben tener una licencia Intune válida. Para obtener más información, consulte Licencias de Microsoft Intune.

- Si sincroniza su Active Directory local con Entra ID, la UPN de Active Directory local de los usuarios debe coincidir con su UPN de Entra ID.
- Los usuarios se deben añadir a UEM como usuarios del directorio.
- Los usuarios deben tener la aplicación Microsoft Authenticator y el UEM Client instalados en sus dispositivos.

1. En la barra de menús de la consola de administración de UEM, haga clic en **Configuración > Integración externa > Acceso condicional de Azure Active Directory**.
2. Haga clic en +.
3. Escriba un nombre para la configuración.
4. En la lista desplegable **Nube de Azure**, haga clic en **GLOBAL**.
5. En el campo **ID de inquilino de Azure**, escriba el nombre de inquilino de su empresa en formato FQDN o el ID de inquilino único en formato GUID.
6. En **Anulación de asignación de dispositivos**, haga clic en **UPN** o **Correo electrónico**.

   Si selecciona UPN, debe comprobar que el inquilino de Entra ID y todos los directorios asignados compartan el mismo valor de UPN para los usuarios antes de guardar la conexión. Después de guardar la conexión, no se puede cambiar la anulación de asignación de dispositivos.
7. En la lista **Directorios de empresas disponibles**, seleccione y añada los directorios de empresas adecuados.
8. Haga clic en **Guardar**.
9. Seleccione la cuenta de administrador que desea utilizar para iniciar sesión en el inquilino de Entra de la empresa.
10. Acepte la solicitud de permiso de Microsoft.
11. En la barra de menús, haga clic en **Políticas y perfiles > Política > BlackBerry Dynamics**. Realice los siguientes pasos para cualquier perfil de BlackBerry Dynamics que tenga previsto asignar a los usuarios de dispositivos (por ejemplo, el perfil predeterminado y cualquier perfil personalizado).
    a) Abra y edite el perfil.
    b) Seleccione **Activar UEM Client para que pueda inscribirse en BlackBerry Dynamics**.
    c) Haga clic en **Guardar**.
    d) Asigne el perfil a los usuarios y grupos según sea necesario.
12. En la barra de menús, haga clic en **Políticas y perfiles > Redes y conexiones > Conectividad de BlackBerry Dynamics**. Realice los siguientes pasos para cualquier perfil de conectividad de BlackBerry Dynamics que tenga previsto asignar a los usuarios de dispositivos (por ejemplo, el perfil predeterminado y cualquier perfil personalizado).
    a) Abra y edite el perfil.
    b) En la sección **Servidores de aplicación**, haga clic en **Agregar**.
    c) Busque y haga clic en **Función-Acceso condicional de Azure**.
    d) Haga clic en **Guardar**.
    e) En la tabla **Acceso condicional de Azure**, haga clic en +.
    f) En el campo **Servidor**, escriba `gdas-<UEM_SRP_ID>.<region_code>.bbsecure.com`.
    g) En el campo **Puerto**, escriba 443.
    h) En **Tipo de ruta**, haga clic en **Directo**.
    i) Haga clic en **Guardar**.
    j) Asigne el perfil a los usuarios y grupos según sea necesario.
13. Asigne la aplicación **Función-Acceso condicional de Azure** a usuarios o grupos. Para obtener más información, consulte Administrar cuentas de usuario y Administrar un grupo de usuarios.

Después de terminar:

- Cuando un usuario activa su dispositivo, se le solicita que se registre con acceso condicional de Active Directory. Se solicita a los usuarios con dispositivos activados que se registren con acceso condicional de Active Directory la siguiente vez que abran UEM Client.
- Cuando se elimina un dispositivo de UEM, el dispositivo permanece registrado para el acceso condicional de Entra ID. Los usuarios pueden eliminar su cuenta de Entra ID de la configuración de la cuenta en la aplicación Microsoft Authenticator, o puede eliminar el dispositivo del portal Entra.

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 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 administración.

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 administración. 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 UEM. Si registra un nuevo certificado APN, los usuarios de dispositivos deberán reactivar los dispositivos para recibir datos.

Se recomienda acceder a la consola de administración y al portal de certificados de inserción de Apple utilizando Google Chrome o Safari, ya que estos navegadores proporcionan una compatibilidad óptima para solicitar y registrar un certificado APN.

Solicitud y registro de un certificado APN

1. En la barra de menús de la consola de administración, haga clic en **Configuración > Integración externa > Apple Push Notification**.
2. En la sección **Paso 1 de 3: Descargar el certificado CSR firmado de BlackBerry**, haga clic en **Descargar certificado**.
3. Guarde el archivo CSR firmado en el ordenador.
4. En la sección **Paso 2 de 3: Solicitar un certificado APN de Apple**, haga clic en **Portal de certificados de inserción de Apple**.
5. Inicie sesión en el portal de certificados de inserción de Apple a través de un ID de Apple válido.
6. Siga las instrucciones para cargar la CSR firmada.

   Si aparece un error de tipo de archivo no válido, puede cambiar el nombre del archivo a un archivo .txt y cargarlo de nuevo.
7. Descargue y guarde el certificado APN en SU equipo.
8. En la sección **Paso 3 de 3: Registrar el certificado APN** de la consola de administración, haga clic en **Examinar**.
9. Navegue y seleccione el certificado APN.
10. Haga clic en **Submit**.

Después de terminar:

- Para probar la conexión entre UEM y el servidor de APN, haga clic en **Probar certificado APN**.
- El certificado APN es válido durante un año. Deberá renovar anualmente el certificado de APN antes de que caduque, a través del mismo ID de Apple que utilizó para obtener el certificado APN original. Para renovar el certificado, repita los pasos anteriores, pero haga clic en **Renovar certificado** en el paso 2.

Solución de problemas: APN

Problema	Solución posible
Cuando intenta obtener una CSR firmada, se muestra el siguiente error: "El sistema ha detectado un error". Intente nuevamente”.	Consulte KB 37266.
Cuando se intenta registrar el certificado APN, se recibe el error "El certificado APN no coincide con la CSR".	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.
No puede activar dispositivos de iOS o macOS.	Es posible que el certificado APN no esté registrado correctamente. Compruebe lo siguiente: • En la barra de menús de la consola de administración, haga clic en **Configuración > Integración externa > Apple Push Notification**. Compruebe que el estado del certificado APN sea "Instalado". Si el estado no es correcto, intente registrar el certificado APN de nuevo. • 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

Puede configurar BlackBerry UEM para que se sincronice con el Programa de inscripción de dispositivos (DEP) de Apple si desea utilizar la consola de administración UEM para administrar la activación de los dispositivos iOS que su empresa adquirió para DEP.

1. En la consola de administración, vaya a **Configuración > Integración externa > Programa de inscripción de dispositivos de Apple**.

   Si utiliza UEM local, haga clic en + y escriba un nombre para la cuenta.
2. En la sección **1 de 4: Crear una cuenta de Apple DEP**, haga clic en **Crear una cuenta de Apple DEP**.
3. Complete los campos y siga las instrucciones para crear su cuenta.
4. En la sección **2 de 4: Descargar una clave pública**, haga clic en **Descargar clave pública**.
5. Guarde la clave pública en el equipo local.
6. En la sección **3 de 4: Generar el identificador del servidor desde la cuenta de Apple DEP**, haga clic en **Abra el portal de Apple DEP**.
7. Inicie sesión en su cuenta de DEP y siga las indicaciones para generar un token de servidor.
8. En la sección **4 de 4: Registrar el identificador del servidor con BlackBerry UEM**, haga clic en **Examinar**.
9. Acceda al archivo de token de servidor .p7m y selecciónelo. Haga clic en **Abrir** y, a continuación, en **Siguiente**.
10. En la ventana de configuración de inscripción, escriba un nombre para la configuración.
11. Si desea que UEM asigne automáticamente la configuración de inscripción a los dispositivos cuando los registra con DEP Apple, seleccione la casilla de verificación **Asignar automáticamente todos los nuevos dispositivos a esta configuración**. No seleccione esta opción si desea utilizar la consola de administración UEM para asignar manualmente la configuración de inscripción a dispositivos específicos.
12. Opcionalmente, escriba el nombre de un departamento y un número de teléfono de soporte para que se muestren en los dispositivos durante la instalación.
13. En la sección **Configuración del dispositivo**, seleccione entre las siguientes opciones:

    - **Permitir emparejamiento**: los usuarios pueden emparejar el dispositivo con un equipo.
    - **Obligatorio**: 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**: los usuarios pueden desactivar los dispositivos.
    - **Espere hasta que el dispositivo esté configurado**: los usuarios no pueden cancelar la configuración del dispositivo hasta que la activación con UEM haya finalizado.
14. En la sección **Omitir durante la configuración**, seleccione los elementos que no desea incluir en la instalación del dispositivo:

Opción	Impacto, si se selecciona
Código de acceso	A los usuarios no se les solicita que creen un código de acceso del dispositivo.
Servicios de ubicación	Los servicios de ubicación están desactivados en el dispositivo.
Restaurar	Los usuarios no pueden restaurar datos desde un archivo de copia de seguridad.
Mover desde Android	Los datos no se pueden restaurar desde un dispositivo Android.
ID de Apple	Se impide que los usuarios inicien sesión en ID de Apple y iCloud.

Opción	Impacto, si se selecciona
Términos y condiciones	Los usuarios no ven los términos y condiciones de iOS.
Siri	Siri está desactivado en los dispositivos.
Diagnostics	La información de diagnóstico no se envía automáticamente desde el dispositivo durante la instalación.
Biométrico	Los usuarios no pueden configurar Touch ID.
Pago	Los usuarios no pueden configurar Apple Pay.
Zoom	Los usuarios no pueden configurar Zoom.
Configuración del botón Inicio	Los usuarios no pueden ajustar el clic del botón Inicio.
Tiempo de pantalla	La opción para configurar el tiempo de pantalla se omitirá durante la inscripción en DEP.
Actualización de software	Los usuarios no ven la pantalla de actualización de software obligatoria en el dispositivo.
iMessage y FaceTime	Los usuarios no ven las pantallas iMessage y FaceTime en el dispositivo.
Tono para mostrar	Los usuarios no verán la pantalla de Tono para mostrar en el dispositivo.
Privacidad	Los usuarios no verán la pantalla Privacidad en el dispositivo.
Integración	Los usuarios no verán la pantalla informativa de integración en el dispositivo.
Migración de Watch	Los usuarios no verán la pantalla de migración de Watch en el dispositivo.
Configuración SIM	Los usuarios no verán la pantalla para configurar un plan móvil en el dispositivo.
Migración de dispositivo a dispositivo	Los usuarios no verán la pantalla de migración de dispositivo a dispositivo en el dispositivo.

15. Haga clic en **Guardar**. 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 Activación de los dispositivos iOS que están inscritos en DEP.
- 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. Para renovar el token, en **Configuración > Integración externa >**

Programa de inscripción de dispositivos de Apple, haga clic en la cuenta DEP y en **Actualizar identificador del servidor**. Complete ambos pasos para generar un nuevo token de servidor y registrarlo con UEM.

- Puede quitar cualquier conexión DEP que cree. Si elimina todas las conexiones DEP, no podrá activar nuevos dispositivos Apple DEP. Si se ha asignado configuraciones de inscripción a los dispositivos y no se han aplicado, UEM elimina las configuraciones de inscripción asignadas a los dispositivos. La eliminación de la conexión no afecta a los dispositivos que están activados en UEM.

Configuración de BlackBerry UEM para que admita dispositivos Android Enterprise

Los dispositivos Android Enterprise proporcionan un nivel de seguridad adicional para las empresas que deseen gestionar dispositivos Android. La tabla siguiente resume las diferentes opciones para la configuración de BlackBerry UEM para la compatibilidad con dispositivos Android Enterprise:

Método	Cuándo se debe elegir este método	Tipo de cuenta de usuario	Servicios de Google compatibles
Conectar un dominio UEM a un dominio Google Workspace.	Su organización utiliza un dominio Google Workspace.	Cuentas de Google Workspace (para empresas)	• Todos los servicios de Google Workspace, como Gmail, Google Calendar y Drive • Gestión de aplicaciones a través de Google Play
Conectar un dominio UEM a un dominio Google Cloud.	Su organización utiliza un dominio Google Cloud.	Cuentas de Google Cloud, también conocidas como cuentas de Google gestionadas (para empresas)	• Similar a Google Workspace, pero sin acceso a productos de pago como Gmail, Google Calendar y Drive • Gestión de aplicaciones a través de Google Play
Permitir que UEM administre dispositivos Android Enterprise como cuentas administradas de Google Play.	Su empresa no utiliza un dominio de Google ni un dominio Google que ya esté conectado a un dominio de UEM y desea utilizar dispositivos Android Enterprise en un segundo dominio de UEM.	Dispositivos Android Enterprise que hayan administrado cuentas de Google Play	• Gestión de aplicaciones a través de Google Play • Los servicios de Google no son compatibles

Configurar BlackBerry UEM para que sea compatible con dispositivos Android Enterprise

Antes de empezar: Si anteriormente ha conectado un dominio UEM a un dominio Google y desea conectar un nuevo dominio UEM, debe quitar la conexión existente. En la barra de menús de la consola de administración, haga clic en **Configuración > Integración externa > Conexión de dominio de Google** y elimine la conexión. También puede eliminar la conexión de la Configuración de administración en Google Play (https://play.google.com/work) con la misma cuenta de Google que utilizó para crear la conexión. Cuando se elimina una conexión, se desactivan todos los dispositivos que se han activado con un tipo de activación Android Enterprise.

1. En la barra de menús de la consola de administración, haga clic en **Configuración > Integración externa > Administración de Android y Chrome**.
2. Lleve a cabo una de estas acciones:

Tarea	Pasos
Use dispositivos Android Enterprise que tengan cuentas de Google Play administradas.	**a.** Seleccione **Permitir que BlackBerry UEM gestione cuentas de Google Play**. **b.** Haga clic en **Siguiente**. **c.** En la ventana **Utilizar Android en el trabajo**, inicie sesión con una cuenta de Google, Google o 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**.
Utilice un dominio de Google.	**a.** Seleccione **Conectar BlackBerry UEM a su dominio de Google existente**. Tenga en cuenta que no puede compartir dominios de Google entre varios dominios de UEM. Esta opción es compatible con Android Enterprise y Chrome OS Enterprise. **b.** Haga clic en **Siguiente**. **c.** Complete los campos para crear una cuenta de servicio y haga clic en **Siguiente**.

3. Lleve a cabo una de estas acciones:
   - Para enviar los detalles de configuración de la aplicación mediante BlackBerry Infrastructure, seleccione **Enviar configuración de la aplicación mediante UEM Client**.
   - Para enviar los detalles de configuración de la aplicación mediante la infraestructura Google, seleccione **Enviar configuración de la aplicación mediante Google Play**.
4. Cuando se le solicite, haga clic en **Aceptar** para aceptar el conjunto de permisos para todas o algunas de las aplicaciones Google y BlackBerry que se muestran.
5. Haga clic en **Hecho**.

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 Android en el contenido de Administración.
- Puede editar la conexión de dominio de **Google en Configuración > Integración externa** para cambiar el tipo de dominio de Google que usa o para probar la conexión de dominio.
- Si alguna vez planea retirar un dominio de UEM que está conectado a Google, elimine la conexión antes de retirar el dominio (**Configuración > Integración externa > Conexión de dominio de Google**). También puede eliminar la conexión de la Configuración de administración en Google Play (https://play.google.com/work) con la misma cuenta de Google que utilizó para crear la conexión. Cuando se elimina una conexión, se desactivan todos los dispositivos que se han activado con un tipo de activación Android Enterprise.

Configuración de BlackBerry UEM para que admita dispositivos Android Management

Los dispositivos Android Management proporcionan seguridad adicional para las empresas que deseen gestionar dispositivos con la API Android Management.

Antes de activar dispositivos con tipos de activación Android Management, revise las Consideraciones sobre los tipos de activación de la administración de Android.

Configurar Android Management en la consola Google Cloud

Debe configurar Android Enterprise con una cuenta Google Play administrada para poder acceder a la opción para configurar Android Management.

Al configurar Android Management, debe utilizar una dirección de correo electrónico dedicada. No puede utilizar la misma dirección de correo electrónico que se utilizó para configurar Android Enterprise.

Antes de empezar: Compruebe que Android Enterprise ya se haya configurado en UEM. Consulte Configuración de BlackBerry UEM para que admita dispositivos Android Enterprise.

1. Vaya a https://console.developers.google.com e inicie sesión con la dirección de correo electrónico que se utilizará para Android Management.
2. En Cloud Console, haga clic en **Nuevo proyecto**.
3. Haga clic en **API y servicios > Seleccionar biblioteca**.
4. En la barra de búsqueda, busque Android Management.
5. En la lista de resultados de búsqueda, active la **API de administración de Android** y la **API Pub/Sub de Cloud**.
6. En la barra de menús de Cloud Console, haga clic en **IAM y administración > Cuentas de servicio > Seleccionar > Crear cuenta de servicio**.
7. En la sección **Conceder acceso a esta cuenta de servicio al proyecto**, en la lista desplegable **Rol**, seleccione **Usuario de administración de Android**.
8. En la segunda lista desplegable **Rol**, seleccione **Admin de Pub/Sub**.
9. En la sección **Conceder acceso a los usuarios a la cuenta de servicio**, introduzca la dirección de correo electrónico que se utilizó en el paso 1.
10. Haga clic en **Hecho**.
11. En la barra de menús, haga clic en **Cuentas de servicio** y seleccione la cuenta que ha creado.
12. Haga clic en **Claves > Añadir clave**.
13. En el cuadro de diálogo **Crear una clave privada para** "<*service_account_name*>", seleccione **JSON**. Haga clic en **Crear**.
14. Anote el nombre de la cuenta de servicio, la dirección de correo electrónico del administrador de la cuenta de servicio y la clave privada JSON.

Después de terminar: Configuración de Android Management en BlackBerry UEM.

Configuración de Android Management en BlackBerry UEM

Antes de empezar:

- Configurar Android Management en la consola Google Cloud.

- Compruebe que tiene el nombre de la cuenta de servicio Android Management, la dirección de correo electrónico del administrador de la cuenta de servicio y la clave privada JSON.

1. En la barra de menús de la consola de administración de UEM, haga clic en **Configuración > Integración externa > Administración de Android y Chrome**.
2. Haga clic en **Agregar una conexión de Administración de Android**.
3. En el campo **Nombre para mostrar de empresa**, introduzca el nombre de la cuenta de servicio.
4. En el campo **Dirección de correo electrónico del administrador**, introduzca la dirección de correo electrónico de la cuenta de servicio.
5. En el campo **Información de cuenta del servicio (formato json)**, introduzca la clave privada JSON.
6. Haga clic en **Guardar**.
7. En el cuadro de diálogo **Nombre de dominio o Nombre de empresa**, en el campo **Su respuesta**, escriba el nombre de la cuenta de servicio de Android Management. Haga clic en **Siguiente**.

Ampliación de la gestión de dispositivos Chrome OS a BlackBerry UEM

Puede integrar BlackBerry UEM con un dominio administrado por Google para ampliar algunas funciones de administración de Chrome OS a UEM. El dominio Google debe incluir la actualización de Chrome Enterprise. Tenga en cuenta que la inscripción y parte de la gestión de los dispositivos Chrome OS se siguen realizando a través de la consola de dominio gestionado de Google.

UEM sincroniza unidades de organización de la consola de administración de Google en grupos de unidades de organización de UEM. Después de la sincronización inicial, UEM se registra con el dominio Google para que se notifique cualquier cambio en las unidades de organización, los usuarios o los dispositivos. Cuando se notifica un cambio a UEM, la base de datos se sincroniza y actualiza en consecuencia.

Paso	Acción
1	Creación de una cuenta de servicio para autenticar con el dominio de Google.
2	Activación de UEM para sincronizar los datos de Chrome OS.
3	Integración de UEM con el dominio Google.

Si ya ha configurado UEM para que sea compatible con los dispositivos Android Enterprise, puede seguir estos pasos para permitir que UEM administre los dispositivos Chrome OS:

Paso	Acción
1	Asegúrese de que el dominio Google de su empresa tenga Chrome OS habilitado para la empresa.
2	Asegúrese de que la API de política de Chrome esté habilitada en el dominio Google de su empresa. Para obtener más información, consulte Creación de una cuenta de servicio para autenticar con el dominio de Google.
3	Asegúrese de que se hayan añadido todos los ámbitos. Para obtener más información, consulte Activación de UEM para sincronizar los datos de Chrome OS.
4	Active la administración de Chrome OS en la consola UEM. Para obtener más información, consulte Integración de UEM con el dominio Google.

Creación de una cuenta de servicio para autenticar con el dominio de Google

Lleve a cabo estos pasos solo si BlackBerry UEM no está conectado a un dominio gestionado Google existente.

1. Inicie sesión en la consola para desarrolladores de Google con la cuenta de Google que desea utilizar para administrar el proyecto.
2. Cree un proyecto.
3. Seleccione el proyecto y cree una cuenta de servicio.
4. Asigne el rol **Básico > Editor** a la cuenta del servicio.
5. Seleccione la cuenta de servicio y añada una nueva clave P12.
6. Copie la contraseña de clave privada y guarde el certificado en el equipo local.
7. Localice el ID único de cliente y la dirección de correo electrónico de la cuenta del servicio y cópielos.
8. En la sección de API y servicios habilitados, busque y habilite las siguientes API:
   - **API de Administrar SDK**
   - **EMM API de Google Play**
   - **API de política de Chrome**

Después de terminar: Activación de UEM para sincronizar los datos de Chrome OS.

Activación de UEM para sincronizar los datos de Chrome OS

Debe utilizar la consola de administración de Google de su empresa para activar las API adicionales que permitirán a UEM sincronizar los datos de Chrome OS.

Antes de empezar: Creación de una cuenta de servicio para autenticar con el dominio de Google.

1. Inicie sesión en la consola de administración de Google con la cuenta de administrador de su dominio de Google.
2. Vaya a la sección de integraciones de terceros para dispositivos móviles.
3. Compruebe que la gestión móvil de terceros de Android esté activada.
4. En la sección para añadir proveedores de EMM, genere un token.
5. Copie el token.
6. En la sección de controles de API de seguridad, haga clic en la opción para administrar la delegación en todo el dominio.
7. Añada una nueva configuración.
8. Para el ID de cliente, pegue el ID de cliente único para la cuenta de servicio de Google.
9. Para los ámbitos OAuth, escriba o pegue lo siguiente en una lista delimitada por comas:
   - https://www.googleapis.com/auth/admin.directory.user
   - https://www.googleapis.com/auth/admin.directory.customer
   - https://www.googleapis.com/auth/admin.directory.customer
   - https://www.googleapis.com/auth/admin.directory.device.mobile
   - https://www.googleapis.com/auth/admin.directory.device.mobile
   - https://www.googleapis.com/auth/admin.directory.user
   - https://www.googleapis.com/auth/admin.directory.device.mobile
   - https://www.googleapis.com/auth/admin.reports.audit.readonly
10. Autorice la conexión.

Después de terminar: Integración de UEM con el dominio Google.

Integración de UEM con el dominio Google

Antes de empezar: Activación de UEM para sincronizar los datos de Chrome OS.

1. Inicie sesión en la consola de administración de UEM con una cuenta de administrador de seguridad.
2. En la barra de menús, haga clic en **Configuración > Integración externa > Administración de Android y Chrome**.
3. Seleccione **Conectar BlackBerry UEM a su dominio de Google existente**.
4. En **Cómo se envía la configuración de la aplicación**, seleccione **Enviar configuración de la aplicación mediante Google Play**.
5. Haga clic en **Siguiente**.
6. En el campo **Contraseña de clave privada**, pegue la contraseña de clave privada que ha copiado de la consola de desarrolladores de Google.
7. Haga clic en **Examinar**.
8. Desplácese hasta el archivo de certificado y selecciónelo en la consola de desarrolladores de Google.
9. En el campo **Dirección de correo electrónico de la cuenta de servicio**, pegue la dirección de correo de la cuenta de servicio de Google de la consola de desarrolladores de Google.
10. En el campo **Dirección de correo electrónico para el administrador de Google**, escriba la dirección de correo electrónico de la cuenta de administrador que se utiliza para gestionar el dominio de Google Cloud o de Google Workspace by Google.
11. En el campo **Token**, pegue el token que se ha generado.
12. En la sección **Seleccionar el tipo de dominio para gestionar los dispositivos Android con un perfil de trabajo**, seleccione si tiene un dominio de Google del tipo correcto.
13. Si selecciona un **dominio de Google Cloud**, seleccione una de las siguientes opciones:
    - **No permitir que BlackBerry UEM cree usuarios en el dominio**: si elige esta opción, debe crear usuarios en su dominio de Google Cloud y crear usuarios locales con las mismas direcciones de correo electrónico en UEM.
    - **Permitir que BlackBerry UEM cree usuarios en el dominio**, si elige esta opción, seleccione una de las siguientes opciones:
      - **No permitir que BlackBerry UEM elimine usuarios en el dominio de Google**
      - **Permitir que BlackBerry UEM elimine usuarios en el dominio de Google**
14. Haga clic en **Siguiente** y seleccione las aplicaciones que desea agregar a UEM.
15. Haga clic en **Siguiente**.
16. Vuelva a hacer clic en **Siguiente**.

Después de terminar: Para sincronizar UEM con la consola de administración Google, en la barra de menús, haga clic en **Configuración > Integración externa > Administración de Android y Chrome**. En la sección **Administración de Chrome OS**, haga clic en **Activar**. UEM realiza una sincronización inicial de datos en 10 minutos y programa sincronizaciones a intervalos regulares. Una vez finalizada la sincronización, puede utilizar las opciones de esta pantalla para iniciar sincronizaciones fuera de la programación para unidades de organización, usuarios y dispositivos.

Simplificación de activaciones de Windows 10

Cuando un usuario activa un dispositivo Windows 10 con BlackBerry UEM, debe especificar la dirección del servidor UEM. Los siguientes métodos ayudan a simplificar el proceso de activación para los usuarios:

Método	Descripción
Integrar UEM con la combinación de Entra ID.	Si se configura la combinación de Entra ID, los usuarios pueden activar sus dispositivos utilizando solo su nombre de usuario y la contraseña de Entra ID. Se requiere una licencia premium de Entra ID. Consulte Integración de UEM con la combinación de Entra ID.
Configure Windows Autopilot.	Cuando se configura Windows Autopilot, la inscripción forma parte de la experiencia de configuración inicial y el dispositivo se activa automáticamente cuando el usuario la completa utilizando únicamente su nombre de usuario y contraseña de Entra ID. Se requiere la integración con la combinación de Entra ID y una licencia premium de Entra ID. Consulte Configuración de Windows Autopilot para la activación de dispositivos.
Implementar un servicio de detección.	Puede utilizar una aplicación web Java de BlackBerry como servicio de detección. Puede utilizar diferentes sistemas operativos y herramientas de aplicación web para implementar un servicio de detección de aplicaciones web. Consulte Implementación de un servicio de detección para simplificar las activaciones Windows 10.

Integración de UEM con la combinación de Entra ID

Puede integrar BlackBerry UEM con la combinación de Entra ID para disfrutar de un proceso de inscripción simplificada para los dispositivos Windows 10. Cuando está configurado, los usuarios pueden inscribir sus dispositivos con UEM usando su nombre de usuario y contraseña de Entra ID. La combinación de Entra ID también requiere de la compatibilidad con Windows Autopilot, que permite que los dispositivos Windows 10,se activen automáticamente con UEM durante la configuración rápida inicial de Windows 10. Se puede instalar un certificado de UEM manualmente en el dispositivo, o los administradores pueden implementar el certificado mediante SCCM.

Antes de empezar: Necesitará la URL de los términos de uso de MDM, la URL de detección de MDM y la URI de ID de aplicación para completar los pasos que se indican a continuación. Para determinar estas URL, en la consola de administración de UEM, cree una cuenta de usuario de prueba y envíe al usuario un correo electrónico de activación mediante la plantilla de correo electrónico de activación predeterminada. La plantilla predeterminada contiene la variable %ClientlessActivationURL% que se resuelve en el valor adecuado en el correo electrónico recibido. Utilice ese valor para las siguientes URL en los pasos siguientes:

- URL de los términos de uso de MDM: *%ClientlessActivationURL%*/Azure/termsofuse
- URL de detección de MDM: *%ClientlessActivationURL%*/Azure/discovery
- URI de ID de aplicación: *%ClientlessActivationURL%*

1. Inicie sesión en el portal de administración de Microsoft Entra ID.

2. En la sección de gestión de MDM y MAM, añada una aplicación de MDM local y asígnele un nombre descriptivo (por ejemplo, `BlackBerry UEM`).
3. Haga clic en la aplicación que ha añadido para configurar sus ajustes.
4. Especifique el alcance del usuario. Si procede, seleccione grupos.
5. Especifique la URL de los términos de uso de MDM y la URL de detección de MDM.
6. Guarde los cambios.
7. En las propiedades de la configuración de la aplicación MDM local, especifique el URI del ID de aplicación.
8. Guarde.

Después de terminar: De forma opcional, Configuración de Windows Autopilot para la activación de dispositivos.

Configuración de Windows Autopilot para la activación de dispositivos

Si configura Windows Autopilot, el dispositivo se activa automáticamente cuando el usuario completa la configuración inmediata solo con su nombre de usuario y contraseña de Entra ID.

Antes de empezar: Integración de UEM con la combinación de Entra ID.

1. Inicie sesión en el portal de administración de Microsoft Entra ID.
2. En la sección de inscripción de dispositivos de Windows, cree un perfil de implementación de Windows Autopilot.
3. Introduzca un nombre y una descripción para el perfil.
4. Configure la configuración rápida inicial.
5. Asigne el perfil a los grupos de usuarios correspondientes.
6. Guarde el perfil.
7. Realice los pasos siguientes en cada dispositivo Windows 10 que desee activar con Windows Autopilot:
   a) Encienda el dispositivo para cargar la configuración inmediata y conéctelo a una red Wi-Fi.
   b) Presione CTRL + MAYÚS + F3 para reiniciar y entrar en el modo auditoría.
   c) Ejecute Windows PowerShell como administrador y ejecute los siguientes comandos:

```
Save-Script -Name Get-WindowsAutoPilotInfo -Path C:\Windows\Temp
```

```
Install-Script -Name Get-WindowsAutoPilotInfo
```

```
Get-WindowsAutoPilotInfo.ps1 -OutputFile C:\Windows\Temp\MyComputer.csv
```

   d) Recopile el archivo .csv resultante de cada dispositivo.
8. En el portal de administración de Microsoft Entra ID, en la sección de inscripción de dispositivos de Windows y dispositivos Windows Autopilot, importe el archivo .csv de cada dispositivo.
9. En el cuadro de diálogo Herramienta de preparación del sistema, realice estas acciones:
   a) En la acción de limpieza del sistema, seleccione la opción para acceder a la experiencia inmediata del sistema (OOBE) y anule la selección de generalizar.
   b) En las opciones de apagado, seleccione la opción de reiniciar.

Implementación de un servicio de detección para simplificar las activaciones 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.

Puede utilizar diferentes sistemas operativos y herramientas de aplicación web para implementar un servicio de detección de aplicaciones web. Los pasos siguientes abordan las tareas de alto nivel; las acciones específicas dependen del entorno de su empresa.

1. Configure una dirección IP estática para el equipo que alojará el servicio de detección.
2. Si desea permitir que los usuarios activen dispositivos mientras están fuera de la red de la empresa, configure el equipo que alojará el servicio de detección para que lo detecte externamente a través del puerto 443.
3. Cree un registro de host A DNS estático para el nombre **enterpriseenrollment.**<***email_domain***> que apunta a la dirección IP estática que ha configurado.
4. Crear e instalar un certificado para proteger las conexiones TLS entre los dispositivos Windows 10 y el servicio de detección.
5. Inicie sesión en myAccount para descargar la herramienta de autodetección de proxy. Ejecute el archivo .exe para extraer un archivo .war.
   El archivo .exe extraerá el archivo `W10AutoDiscovery-<version>.war` en `C:\BlackBerry`.
6. Cambie el nombre de `W10AutoDiscovery-<version>.war` a `ROOT.war`. Muévalo a la carpeta raíz del servidor de aplicaciones Java.
7. Actualice el archivo wdp.properties de la aplicación web del servicio de detección para incluir una lista de los ID de SRP (UEM local) o los ID de inquilino (UEM Cloud) para sus instancias de UEM. Puede encontrar los ID en myAccount.

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 un servidor local de origen de UEM. En entornos UEM locales, también puede migrar desde un servidor Good Control independiente.

Paso	Acción
1	Revise los requisitos previos y las prácticas recomendadas y consideraciones de la migración.
2	Conexión con un servidor de origen.
3	Migración de políticas de TI, perfiles y grupos desde un servidor de origen.
4	Migración de usuarios desde un servidor de origen.
5	Migración de dispositivos desde un servidor de origen.

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

Elemento	Requisitos previos
Permisos del administrador de seguridad	Siga las instrucciones de esta sección como administrador de seguridad.
Versiones compatibles del servidor de origen	Para entornos locales de UEM, puede migrar desde los siguientes servidores de origen: • UEM local 12.15 o posterior • Good Control (independiente) 5.0 o posterior Para UEM Cloud, solo puede migrar datos desde el entorno local de UEM. La instancia local de origen de UEM debe ser una de las tres versiones principales más recientes. Las versiones anteriores no son compatibles con la migración.
BlackBerry Connectivity Node (solo UEM Cloud)	Para admitir todas las funciones de migración, debe activar al menos una BlackBerry Connectivity Node versión 2.13 o posterior.

Elemento	Requisitos previos
Conexión del directorio de la empresa UEM	Configure la conexión con el directorio de la empresa de destino UEM de la misma forma en que está configurada en el servidor de origen. La migración no funciona si la conexión del directorio de la empresa no coincide.
Desfragmentación de las bases de datos (solo UEM local)	Desfragmente las bases de datos de origen y de destino de UEM antes de comenzar la migración. Si está migrando un gran número de usuarios o dispositivos, debería desfragmentar la base de datos de destino de UEM después de migrar cada grupo de usuarios o dispositivos.
BlackBerry UEM Client	• UEM local: si tiene previsto migrar las aplicaciones de UEM Client y BlackBerry Dynamics inscritas en BlackBerry Dynamics, la última UEM Client debe estar instalada en los dispositivos. • UEM Cloud: UEM Client debe tener la versión 12.x o posterior.
Aplicaciones de BlackBerry Dynamics	• UEM local: todas las aplicaciones de BlackBerry Dynamics que tenga previsto migrar deben utilizar SDK versión BlackBerry Dynamics 7.1 o posteriores. Para las migraciones desde Good Control, las aplicaciones deben usar SDK versión 4.0.0 o posteriores. • UEM Cloud: todas las aplicaciones BlackBerry Dynamics que planea migrar deben utilizar SDK BlackBerry Dynamics versión 8.0 o posteriores. • Las aplicaciones BlackBerry Dynamics que no sean compatibles con la migración se borrarán del dispositivo durante el proceso de migración.

Elemento	Requisitos previos
Autorizaciones de las aplicaciones de BlackBerry Dynamics	• El servidor de destino de UEM debe tener la misma lista de autorizaciones de aplicaciones de BlackBerry Dynamics que el servidor de origen. • A todas las cuentas de usuario migradas se les debe asignar la misma lista de autorizaciones de aplicaciones de BlackBerry Dynamics en la instancia de destino de UEM que tienen en el servidor de origen. • El delegado de autenticación debe ser el mismo en el servidor de origen y el servidor de destino. Puede cambiar la delegada de autenticación después de la migración. • Si el perfil BlackBerry Dynamics en el servidor de origen permite que BlackBerry Dynamics active UEM Client, configúrelo de la misma manera en el servidor de destino. • El delegado de autenticación debe ser el mismo en el servidor de origen y el servidor de destino de UEM. Puede cambiar la delegada de autenticación después de la migración. • Para las migraciones desde una instancia de Good Control, no se migrarán los dispositivos con un delegado de autenticación de dispositivos de Good for Enterprise. Después de eliminar Good for Enterprise como delegado de autenticación, actualice la caché antes de continuar con la migración. Si las autorizaciones no coinciden entre el servidor de origen y el de destino, se desactivan las aplicaciones de BlackBerry Dynamics después de la migración.
Aplicaciones BlackBerry Dynamics personalizadas	Las aplicaciones personalizadas solo se migran si los servidores de origen y destino tienen el mismo ID de empresa. Para obtener más información sobre la fusión de organizaciones, consulte KB 47626.
Puertos	• UEM local: asegúrese de que los puertos 1433 (TCP) y 1434 (UDP) no están bloqueados en Microsoft SQL Server. • UEM Cloud: el puerto 8887 (TCP) debe estar abierto entre el servidor de UEM local y BlackBerry Connectivity Node. Asegúrese de que el puerto que utiliza la instancia de Microsoft SQL Server que aloja la base de datos de UEM local está abierto y que se puede acceder a él mediante BlackBerry Connectivity Node (por ejemplo, en el puerto 1433).

Consideraciones y prácticas recomendadas sobre la migración de UEM

Migrar políticas de TI, perfiles y grupos

Elemento	Consideraciones y prácticas recomendadas
Elementos copiados de un servidor UEM de origen	• Políticas de TI seleccionadas • Perfiles de correo electrónico • Perfiles de Wi-Fi • Perfiles VPN • Perfiles de proxy • Perfiles de conectividad de BlackBerry Dynamics • Perfiles de BlackBerry Dynamics • Ajustes de configuración de la aplicación • 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) • Certificados de cliente (uso de aplicaciones) • Las políticas y perfiles asociados a las políticas y los perfiles seleccionados
Elementos copiados de un servidor Good Control de origen a UEM solo local	• Conjuntos de políticas • Perfiles de conectividad • Grupos de aplicaciones • Uso de aplicaciones (para los certificados) • Certificados
Migración de grupo	Las asignaciones de usuarios, roles y configuración de software no se migran. Debe volver a crear manualmente esas asignaciones en el servidor de destino de UEM.
Contraseñas de políticas de TI	Si alguna de las políticas de TI de origen que se seleccionaron para los dispositivos Android tiene una longitud mínima de contraseña inferior a 4 o superior a 16, no se pueden migrar las políticas de TI o los perfiles de UEM. Cambie la política de TI de origen en consecuencia.
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.

Elemento	Consideraciones y prácticas recomendadas
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 UEM. Algunos de los 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 principal y el clúster de BlackBerry Proxy secundario.
Grupos de aplicaciones (Good Control a UEM solo local)	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 UEM.
Uso de certificados (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
Tareas posteriores a la migración para los usuarios de BlackBerry Dynamics	Después de migrar usuarios, dispositivos, grupos y otros datos a Good Control a UEM solo local, o de un servidor local de origen de UEM a UEM Cloud, realice las siguientes tareas: • 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 cumplimiento). • Mueva las configuraciones en archivos .json de Good Control a UEM. • En los perfiles de conectividad migrados, especifique la información de los servidores de aplicaciones y los clústeres BlackBerry Proxy.

Migrar usuarios

Elemento	
Número máximo de usuarios	Puede migrar un máximo de 1000 usuarios a la vez desde un servidor de origen. Si selecciona un número de usuarios superior al máximo, solo se migrará el número máximo; el resto se omitirán. Puede repetir el proceso de migración cuando sea necesario para migrar todos los usuarios del servidor de origen.
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 electrónico en el servidor de destino de UEM. • 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.

Elemento	
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.
BlackBerry UEM Self-Service	• 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. • 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 tenían permiso para acceder a BlackBerry UEM Self-Service antes de la migración no se les concede automáticamente el permiso después de la migración.

Migración de dispositivos desde un servidor de origen

Elemento	Consideraciones y prácticas recomendadas
Validar la configuración	Se recomienda migrar un dispositivo para cada configuración única (por ejemplo, distintos grupos, políticas, configuraciones de aplicaciones, etc.) para asegurarse de que el servidor de destino se configure correctamente antes de migrar el resto de los dispositivos.
Número máximo de dispositivos	Puede migrar un máximo de 2000 dispositivos a la vez desde un servidor de origen.
Usuarios	• Los usuarios de dispositivos deben existir en el dominio de destino de UEM. • Debe migrar todos los dispositivos del usuario al mismo tiempo.
Dispositivos iOS gestionados desde una instancia de origen de UEM	• Los dispositivos deben tener la versión más reciente de UEM Client. • Los dispositivos asignados al perfil de bloqueo de aplicaciones no se pueden migrar porque UEM Client no puede abrirse para la migración. • Los dispositivos DEP Apple sin UEM Client se muestran en la lista de dispositivos que no son compatibles con la migración, pero que se pueden migrar con un método alternativo. Debe realizar pasos adicionales para migrar dispositivos DEP con o sin UEM Client. Consulte Migración de dispositivos DEP desde un servidor de origen. • Los dispositivos de inscripción de usuarios no se pueden migrar. • 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**. Si intenta realizar la migración sin realizar este paso, la aplicación se eliminará y el dispositivo podría desinscribirse de UEM.

Elemento	Consideraciones y prácticas recomendadas
Dispositivos Android gestionados desde una instancia de origen de UEM	• Los dispositivos Android Enterprise deben tener la versión más reciente de UEM Client instalada. • No se pueden migrar los dispositivos Android con un perfil de trabajo que utiliza una cuenta de Google o un dominio de Google.
Dispositivos Chrome OS	Puede migrar los dispositivos Chrome OS desde un servidor de origen de UEM.
Dispositivos que no son compatibles con la migración	• Windows • macOS
Grupo de dispositivos compartidos	No puede migrar un dispositivo que pertenece a un grupo de dispositivos compartidos. Estos dispositivos no aparecen en la lista de migración.
Dispositivos con BlackBerry Dynamics	• 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. • BlackBerry Access for Windows, BlackBerry Access for macOS y BlackBerry Bridge no son compatibles con la migración. Cuando finalice la migración, los usuarios tendrán que volver a inscribir estas aplicaciones. • El proceso de migración no realiza un seguimiento ni garantiza la migración de UEM Client ni de las aplicaciones activadas en un dispositivo después de que los datos del dispositivo se hayan almacenado en caché. Se recomienda actualizar la caché del usuario antes de cada migración. • Los dispositivos con BlackBerry Dynamics siempre están siempre en BlackBerry Dynamics en el servidor de destino. • Para las migraciones desde una instancia (independiente) de Good Control, no se migrarán las inscripciones a MDM de Good Dynamics. • Si un usuario tiene más de un dispositivo con aplicaciones de BlackBerry Dynamics, todos los dispositivos se seleccionan automáticamente para migración. • 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 servidor de origen de UEM. Al finalizar la migración, hay que obtener la clave del servidor de destino de UEM. • 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.

Conexión con un servidor de origen

Para migrar datos, debe conectar BlackBerry UEM al servidor de origen. Solo puede tener un servidor de origen activo a la vez.

Antes de empezar:

- Revise los requisitos previos y las prácticas recomendadas y consideraciones de la migración.
- En los entornos locales de UEM, compruebe que la cuenta de la base de datos asociada a sus credenciales de inicio de sesión tenga permisos de escritura.
- En entornos UEM Cloud, si hay más de un BlackBerry Connectivity Node activado, configure todas las instancias de BlackBerry Connectivity Node para que se conecten a la misma base de datos de origen.

Siga los pasos correspondientes a su tipo de entorno de UEM:

Entorno	Pasos
UEM local	**a.** En la barra de menús de la consola de administración, haga clic en **Configuración > Migración > Configuración**. **b.** Haga clic en +. **c.** En la lista desplegable **Tipo de origen**, haga clic en el tipo de servidor de origen adecuado. **d.** Especifique la información del servidor de origen. Si está migrando datos desde un servidor de origen de Good Control, solo necesita exportar y cargar el certificado si no se ha sustituido por un certificado de terceros. De forma predeterminada, UEM confía en los certificados de proveedores de terceros. **e.** Haga clic en **Probar conexión**. **f.** Haga clic en **Guardar**.
UEM Cloud	**a.** En la barra de menú de la consola de administración de BlackBerry Connectivity Node, haga clic en **Configuración general > Migración**. **b.** Haga clic en +. **c.** Especifique la información del servidor de origen. • Para el campo **Servidor de bases de datos**, utilice el formato *<host>**<instance>* para un puerto dinámico y *<host>*:*<port>* para un puerto estático. • Si selecciona la autenticación NT de Windows, cambie las propiedades de inicio de sesión del servicio BlackBerry UEM - BlackBerry Cloud Connector a la misma cuenta que se utilizó para instalar el servidor de origen. Una vez finalizada la migración, cambie las propiedades de Inicio de sesión para utilizar la cuenta del sistema local. **d.** Haga clic en **Guardar**. **e.** En la consola de administración de UEM, haga clic en **Configuración > Migración > Configuración**. **f.** Haga clic en +. **g.** Escriba el nombre de la base de datos de origen. **h.** Haga clic en **Probar conexión**. **i.** Haga clic en **Guardar**.

Después de terminar: Efectúe una de las acciones siguientes:

- Migración de políticas de TI, perfiles y grupos desde un servidor de origen.
- Migración de usuarios desde un servidor de origen.
- Migración de dispositivos desde un servidor de origen.

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

Antes de empezar: Conexión con un servidor de origen.

1. En la barra de menús de la consola de administración, haga clic en **Configuración > Migración**.

   Si ha configurado más de un servidor de origen en un entorno local UEM, seleccione el servidor de origen desde el que desea migrar los datos.
2. Haga clic en **Políticas de TI, perfiles, grupos**.
3. Haga clic en **Siguiente**.
4. Seleccione los elementos que desea migrar.

   El nombre del servidor de origen se anexa a cada nombre de perfil y política durante la migración al servidor de destino.
5. Haga clic en **Vista previa**.
6. Haga clic en **Migrar**.

Después de terminar:

- 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**.
- 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.
- Migración de usuarios desde un servidor de origen.

Migración de usuarios desde un servidor de origen

Antes de empezar:

- Conexión con un servidor de origen.
- Migración de políticas de TI, perfiles y grupos desde un servidor de origen.

1. En la barra de menús de la consola de administración, haga clic en **Configuración > Migración > Usuarios**.
2. Haga clic en **Actualizar caché**.

   La actualización requiere aproximadamente 10 minutos por cada 1000 usuarios. La actualización de la caché solo es obligatoria para el primer conjunto de usuarios que desea migrar. Si hace cambios en el servidor de origen durante la migración, se recomienda actualizar la caché de nuevo.
3. Haga clic en **Siguiente**.
4. Seleccione los usuarios que desea migrar.

   De forma predeterminada, solo se mostrarán los primeros 20 000 usuarios. Puede buscar usuarios específicos según sea necesario. Tenga en cuenta que, al seleccionar todos los usuarios, solo se seleccionan los que se muestran en la primera página.
5. Haga clic en **Siguiente**.
6. Asigne una política de TI, grupos y perfiles a los usuarios seleccionados.

7. Haga clic en **Vista previa**.
8. Haga clic en **Migrar**.

Tenga en cuenta que las cuentas de usuario migradas no se quitan del servidor de origen.

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

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:

- Conexión con un servidor de origen.
- Migración de políticas de TI, perfiles y grupos desde un servidor de origen.
- Migración de usuarios desde un servidor de origen.
- Para migrar dispositivos DEP, consulte Migración de dispositivos DEP desde un servidor de origen. Utilice las instrucciones que aparecen a continuación para cualquier otro dispositivo.
- Notifique a los usuarios de los dispositivos iOS que deben abrir BlackBerry UEM Client y mantenerlo abierto hasta que se complete la migración.

1. En la barra de menús de la consola de administración, haga clic en **Configuración > Migración > Dispositivos**.
2. Haga clic en **Actualizar caché**.

   La actualización requiere aproximadamente 10 minutos por cada 1000 dispositivos. Actualizar la caché solo es obligatorio para el primer conjunto de dispositivos que se quieran migrar. Si hace cambios en el servidor de origen durante la migración, se recomienda actualizar la caché de nuevo.
3. Haga clic en **Siguiente**.
4. Seleccione los dispositivos que desea migrar.

   De forma predeterminada, solo se mostrarán los primeros 20 000 dispositivos. Puede buscar dispositivos específicos según sea necesario. Tenga en cuenta que al seleccionar todos los dispositivos solo se seleccionan los que se muestran en la primera página.
5. Haga clic en **Vista previa**.
6. Haga clic en **Migrar**.
7. Haga clic en **Migración** > **Estado**.

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

Migración de dispositivos DEP desde un servidor de origen

Puede migrar los dispositivos iOS que están inscritos en el programa de inscripción de dispositivos (DEP) de Apple de un servidor de origen de UEM a otro servidor de destino de UEM. Complete las tareas adicionales que se detallan a continuación para admitir la migración de dispositivos DEP. Después de completar los pasos que se indican a continuación, los dispositivos DEP con el tipo de activación BlackBerry UEM Client y Controles de MDM se pueden migrar mediante la consola de administración UEM. Los dispositivos DEP sin UEM Client o con otros tipos de activación requieren un restablecimiento de fábrica y una reactivación en el servidor de destino.

Tenga en cuenta que la configuración de inscripción de DEP no se migra y que los dispositivos perderán la configuración de inscripción en el entorno de destino.

Antes de empezar: En la consola de administración, haga clic en la opción **Aplicaciones** de la barra de menú. Busque y haga clic en UEM Client. En la pestaña **iOS**, desmarque la casilla de verificación **Eliminar la aplicación**

del dispositivo cuando este se haya eliminado de BlackBerry UEM. Si intenta migrar dispositivos sin desactivar esta opción, la UEM Client se eliminará y podría anularse la inscripción del dispositivo en UEM.

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

   Asegúrese de que el perfil de DEP del servidor de destino de UEM coincida con el perfil de DEP del servidor de origen.
3. Mueva los dispositivos DEP del servidor de MDM virtual de origen al nuevo servidor MDM virtual.
4. Efectúe una de las acciones siguientes:

   - Para los dispositivos DEP con el tipo de activación UEM Client y Controles de MDM, utilice la consola de administración de UEM para migrar los dispositivos al servidor de destino.
   - Para los dispositivos DEP sin UEM Client o con otros tipos de activación, realice un restablecimiento de fábrica de cada dispositivo y reactive el dispositivo en el servidor de destino.

Después de terminar: Para dispositivos DEP con el tipo de activación UEM Client y Controles de MDM, indique a los usuarios que abran la aplicación configurada como delegado de autenticación. Esto activará la migración en el dispositivo.

Configuración de las propiedades y la comunicación de red para las aplicaciones BlackBerry Dynamics

Siga las instrucciones de esta sección para configurar la comunicación de red y otras propiedades de las aplicaciones BlackBerry Dynamics.

Tarea	Descripción
Gestión de clústeres de BlackBerry Proxy.	Crear y administrar clústeres de BlackBerry Proxy que enruten datos para las aplicaciones BlackBerry Dynamics.
Configuración de Direct Connect utilizando el reenvío de puertos.	Configurar Direct Connect para instancias BlackBerry Proxy.
Configuración de las propiedades de BlackBerry Dynamics (Solo local).	Configurar las propiedades de las aplicaciones BlackBerry Dynamics que planea implementar en el entorno de su empresa.
Configuración de los parámetros de comunicación de las aplicaciones de BlackBerry Dynamics (Solo local).	Configurar los ajustes de comunicación para las aplicaciones BlackBerry Dynamics que planea implementar en el entorno de su empresa, incluido el protocolo de comunicación que utilizarán las aplicaciones.
Envío de los datos de aplicaciones de BlackBerry Dynamics a través de un proxy HTTP.	Configurar UEM para enviar datos de aplicaciones de BlackBerry Dynamics a través de un proxy HTTP entre BlackBerry Proxy y un servidor de aplicaciones.
Métodos para enrutar el tráfico para las aplicaciones BlackBerry Dynamics.	Detalles de los diferentes métodos que puede utilizar para enrutar el tráfico de las aplicaciones BlackBerry Dynamics.
Configuración de la autenticación de Kerberos para aplicaciones BlackBerry Dynamics (Solo local).	Configurar la delegación restringida Kerberos o Kerberos PKINIT para simplificar la autenticación de los usuarios.

Para obtener más información acerca de la implementación y administración de aplicaciones BlackBerry Dynamics, consulte Administración 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 añaden nuevas instancias a un clúster de forma predeterminada; las nuevas instancias de clústeres se consideran no asignadas y se deben añadir a uno de los clústeres disponibles de forma manual.

1. En la barra de menús de la consola de administración, haga clic en **Configuración > BlackBerry Dynamics > Clústeres**.
2. 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 **Aceptar**.
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 al que desea añadir la instancia. **c.** Haga clic en **Guardar**.
Elimine un clúster de BlackBerry Proxy vacío.	**a.** Haga clic en × para dicho clúster. **b.** Haga clic en **Eliminar**.
Establezca la configuración de proxy de la aplicación para un clúster.	**a.** Haga clic en el nombre del clúster. **b.** Haga clic en **Anular configuración global** **c.** Consulte Configuración de los parámetros de proxy de la aplicación BlackBerry Dynamics.
Descargue actualizaciones del archivo PAC para todos los clústeres.	Haga clic en **Actualizar caché de PAC**.
Especifique 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 + junto a **Confianzas de servidor PAC**. **d.** Haga clic en **Examinar**. **e.** Navegue al archivo de certificado que desea utilizar y selecciónelo. **f.** Haga clic en **Abrir**. **g.** Escriba una descripción para el certificado. **h.** Haga clic en **Agregar**.
Habilite un BlackBerry Proxy para su uso en la activación (solo UEM local).	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 el 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 Node se instalan en una DMZ, asegúrese de que los puertos correctos estén 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 barra de menús de la consola de administración, haga clic en **Configuración > BlackBerry Dynamics > Direct Connect**.
2. Haga clic en una instancia de BlackBerry Proxy.
3. Para activar Direct Connect, seleccione la casilla de verificación **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.
4. Repítalo 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 Gestión de clústeres de BlackBerry Proxy.
5. Haga clic en **Guardar**.

Configuración de las propiedades de BlackBerry Dynamics

En un entorno UEM local, puede configurar varias propiedades relacionadas con la seguridad, el comportamiento y las comunicaciones de las aplicaciones BlackBerry Dynamics.

1. En la consola de gestión, en la barra de menú, haga clic en **Configuración > BlackBerry Dynamics**.
2. Efectúe una de las acciones siguientes:

Tarea	Pasos
Cambie las propiedades globales de las aplicaciones BlackBerry Dynamics.	• Haga clic en **Propiedades globales**. • Configure las propiedades según sea necesario. Consulte Propiedades globales de BlackBerry Dynamics. • Haga clic en **Guardar**.
Cambie las propiedades BlackBerry Dynamics de un servidor UEM específico.	• Haga clic en **Propiedades**. • En la lista desplegable **Tipo de servidor**, haga clic en **Servidores de BlackBerry Control** y seleccione el servidor de UEM que desea configurar. • Configure las propiedades según sea necesario. Consulte Propiedades de BlackBerry Dynamics. • Haga clic en **Guardar**.

Tarea	Pasos
Cambie las propiedades de una instancia BlackBerry Proxy.	• 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. • Configure las propiedades según sea necesario. Consulte Propiedades de BlackBerry Proxy. • 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.

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, 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 la autenticación del cliente. Esta es una propiedad de solo lectura y no se puede cambiar.	86400	—

Communication

Propiedad	Descripción	Predetermi	Reiniciar
cntmgmt.internal.port	El puerto interno para el servicio de gestión de contenedores.	17317	Sí
cntmgmt.max.conns.above.limit	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

Propiedad	Descripción	Predetermi	Reiniciar
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. Esta es una propiedad de solo lectura y no se puede cambiar.	Activado	—
cntmgmt.ssl.internal.enable	Controla si SSL está habilitado para la gestión interna de contenedores. Esta es una propiedad de solo lectura y no se puede cambiar.	Activado	—

Contenedores duplicados

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

Propiedad	Descripción	Predetermi	Reiniciar
Eliminar automáticamente los contenedores duplicados en un mismo dispositivo del usuario después del aprovisionamiento	Permite especificar si 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

Propiedad	Descripción	Predetermi	Reiniciar
Habilitar trabajo para eliminar automáticamente contenedores duplicados (activado/desactivado)	Permite especificar si 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 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 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 BlackBerry Dynamics usan 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. Puede que el Active Directory de su empresa no admita ambas opciones o que solo funcione con una de ellas, según su entorno.	Desactivado	No
Activar KCD (gc.krb5.enabled)	Permite especificar si 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 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 UEM ejecuta una tarea para identificar y volver a enviar mensajes no confirmados. Si se establece en 0, UEM no ejecuta la tarea.	900	Sí

Propiedad	Descripción	Predetermi	Reiniciar
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 UEM recupera políticas de conformidad para todos los conjuntos de políticas.	1440	Sí

Depurar los contenedores inactivos

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

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 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 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 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
gc.purge.dbJobs Purgar trabajos del servidor	Permite especificar si UEM debe depurar automáticamente trabajos del servidor en intervalos regulares.	Activado	Sí
gc.purge.dbJobs.interval Intervalo de purga de trabajos del servidor	Si "Depurar trabajos del servidor" está activado, la frecuencia, en días, en la que UEM depura trabajos del servidor.	30	Sí

Propiedades de BlackBerry Dynamics

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 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
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 una de las instancias de BlackBerry Proxy de su empresa.

Propiedad	Descripción	Predeterm	Reiniciar
gp.gps.max.sessions	Número máximo de sesiones activas.	15000	—

Propiedad	Descripción	Predeterm	Reiniciar
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.	Desactivad	—
gp.gps.unalias.hostname	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
gps.directconnect.supported.ciphers	Añade o cambia paquetes de cifrado que encriptan los puentes y las comunicaciones hechas a través de BlackBerry Direct Connect. Puede elegir tener su propio servidor proxy configurado para Direct Connect y ubicado entre sus dispositivos de cliente y el servidor BlackBerry Proxy. Si ha añadido su propio servidor proxy, asegúrese de que los cifrados del servidor BlackBerry Proxy se correspondan con los que requiere su propio servidor proxy. Todos los cifrados deben ser compatibles con Java.	Indicado en la interfaz de usuario	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

Propiedad	Descripción	Predeterm	Reiniciar
gp.eacp.command.service.nslookup.srv.ldap	Activa LDAP a través de TCP para los servidores Active Directory. Los servidores Active Directory ofrecen el servicio LDAP a través del protocolo TCP. Para buscar un servidor LDAP, los clientes consultan un registro con el siguiente formato en el DNS: _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.	Desactivad	Sí
gc.mdc.hb.timeout	Permite especificar el tiempo de espera de latido.	0	—
gp.server.secure.ciphers	Añade o cambia paquetes de cifrado que cifran las comunicaciones realizadas a través de un servidor BlackBerry Proxy. Todos los cifrados deben ser compatibles con Java.	Indicado en la interfaz de usuario	—
gp.server.secure.protocols	Añade o cambia los protocolos de cifrado que desea que sean compatibles con el servidor BlackBerry Proxy.	TLSv1.2	—

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

En los entornos UEM locales, 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 barra de menús de la consola de administración, haga clic en **Configuración > BlackBerry Dynamics > Configuración de comunicación**.
2. Ajuste la configuración según sea necesario.
3. 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 la configuración de proxy manual como los archivos PAC para conectarse a servidores 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 UEM. Para obtener más información, consulte la Guía de administración de BlackBerry Access.

Consideraciones para utilizar un archivo PAC con BlackBerry Proxy

Consideraciones	Detalles
Directivas de archivo PAC admitidas	• DIRECTO • PROXY (se consideran conexiones proxy HTTPS establecidas utilizando HTTP CONNECT) • HTTPS (conexiones establecidas utilizando HTTP CONNECT)
Directivas de archivo PAC no compatibles	Se producirá un error de conexión para lo siguiente: • SOCKS • SOCKS4 • SOCKS5 • HTTP • Directiva "NATIVA" personalizada definida por BlackBerry Access Las directivas de archivo de BLOQUE se tratan como DIRECTAS.
Limitaciones	• 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.
Caché de PAC	BlackBerry Proxy descargará y almacenará en caché el archivo PAC para mejorar el rendimiento. La caché de PAC se actualiza cada 24 horas. Si desea actualizar la caché manualmente, vaya a **Configuración > Infraestructura > Enrutador y proxy BlackBerry > Configuración global** en la consola de administración y haga clic en Actualizar caché de PAC.

Configuración de los parámetros de proxy de la aplicación BlackBerry Dynamics

1. Siga el paso adecuado para su entorno UEM:

Entorno	Tarea
UEM local	Haga una de las siguientes tareas en la consola de administración de UEM: • Si desea establecer la configuración global del proxy de aplicaciones, haga clic en **Configuración > Infraestructura > Enrutador y proxy BlackBerry** y expanda **Configuración global**. • Si desea establecer la configuración del proxy de aplicaciones para un clúster, haga clic en **Configuración > BlackBerry Dynamics > Clústeres**. Haga clic en el nombre de un clúster y seleccione la casilla de verificación **Anular configuración global**. • Si desea establecer la configuración manual del proxy de aplicaciones para un servidor, haga clic en **Configuración > Infraestructura > Enrutador y proxy de BlackBerry**. Expanda un servidor y seleccione la casilla de verificación **Anular configuración global**. Tenga en cuenta que los archivos PAC no son compatibles cuando se anula la configuración de proxy general para un servidor.
UEM Cloud	En la consola de administración de BlackBerry Connectivity Node, haga clic en **Configuración general > Enrutador y proxy BlackBerry > Configuración global**.

2. Seleccione la opción adecuada y realice los pasos necesarios:

Opción	Pasos
Activar proxy HTTP manual	**a.** Seleccione la configuración de proxy adecuada. Si desea utilizar el proxy para conectarse a servidores específicos, haga clic en + para añadir servidores. **b.** Especifique la dirección del servidor proxy y el número de puerto en el que escucha. **c.** Si el servidor proxy requiere autenticación, seleccione la casilla de verificación **Usar autenticación** y especifique las credenciales de autenticación.
Activar PAC	En el campo **URL de PAC**, escriba la URL del archivo PAC. Si los proxies especificados en el archivo PAC requieren autenticación, seleccione la casilla de verificación **Admitir autenticación de proxy** y especifique las credenciales de autenticación. Las credenciales de autenticación de usuario final no son compatibles para la autenticación proxy.

3. Haga clic en **Guardar**.

Métodos para enrutar el tráfico para las aplicaciones BlackBerry Dynamics

BlackBerry UEM ofrece varias opciones que le permiten controlar cómo se enruta el tráfico de BlackBerry Dynamics. De forma predeterminada, todo el tráfico de aplicaciones BlackBerry Dynamics se enruta directamente a Internet sin configuraciones de servidor proxy web. En esta sección solo se tratan las configuraciones que afectan al enrutamiento general.

El enrutamiento de las aplicaciones BlackBerry Dynamics se puede cambiar con las siguientes configuraciones:

Configuración	Detalles
Perfil de conectividad BlackBerry Dynamics asignado.	• El único elemento configurado en el perfil de conectividad predeterminado BlackBerry Dynamics es Tipo de ruta de dominio permitido por defecto, que está definido en Directa. • Si se usa el perfil de conectividad predeterminado de BlackBerry Dynamics, las aplicaciones BlackBerry Dynamics no podrán acceder a servidores o dominios internos. Puede modificar el perfil de conectividad predeterminado o crear otro nuevo para autorizar la conectividad con servidores internos. • Para obtener más información, consulte Crear un perfil de conectividad de BlackBerry Dynamics en el contenido de Administración.

Configuración del servidor proxy web de BlackBerry Proxy	• De forma predeterminada, BlackBerry Proxy no está configurado para utilizar un servidor proxy web. Cada servidor BlackBerry Proxy intenta conectarse directamente a Internet para establecer conexiones. Esto se aplica tanto al tráfico del servidor de aplicaciones como a las conexiones de BlackBerry Dynamics NOC.
	• Para obtener información sobre la configuración de BlackBerry Proxy, consulte Envío de los datos de aplicaciones de BlackBerry Dynamics a través de un proxy HTTP.
	• En el perfil de conectividad de BlackBerry Dynamics, puede especificar los servidores a los que las aplicaciones de BlackBerry Dynamics pueden acceder a través del firewall utilizando BlackBerry Proxy. Para obtener más información, consulte Crear un perfil de conectividad de BlackBerry Dynamics en el contenido de Administración.
	• El enrutamiento del tráfico a través de BlackBerry Proxy permite que los navegadores web y las aplicaciones BlackBerry Dynamics de los dispositivos se conecten a cualquier servidor protegido por el firewall al que pueda acceder BlackBerry Proxy, y permite supervisar fácilmente el tráfico de datos entre las aplicaciones BlackBerry Dynamics y los recursos de la empresa.
	• Si decide enrutar datos a través de un servidor BlackBerry Proxy, tenga en cuenta lo siguiente:
	  • 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.
	  • 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.

Configuración	Detalles
Configuración específica de la aplicación	• 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 las aplicaciones de BlackBerry Dynamics para conocer las configuraciones de aplicación que se deben aplicar. • 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. • 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.

Si configura y asigna un perfil de conectividad BlackBerry Dynamics y una configuración de proxy web para los servidores BlackBerry Proxy, el perfil de conectividad 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 proxy web establecida en el servidor BlackBerry Proxy. La configuración de un proxy web en el servidor BlackBerry Proxy controla cómo BlackBerry Proxy gestiona el envío de tráfico a Internet; no afecta a la forma en que la aplicación BlackBerry Dynamics del dispositivo evalúa las conexiones.

Ejemplos de situaciones de enrutamiento para el tráfico BlackBerry Dynamics

Las siguientes situaciones son ejemplos de configuraciones comunes:

Situación	Perfil de conectividad de BlackBerry Dynamics	Configuración de proxy web para BlackBerry Proxy	Configuración específica de la aplicación
Enrutamiento del tráfico a servidores o dominios específicos a través de BlackBerry Proxy. 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 pueda seguir siendo directo.	• Tipo de ruta de dominio permitido por defecto: directa • Dominios permitidos: añada los dominios internos que se deben enrutar a través de BlackBerry Proxy y seleccione un clúster. • Servidores adicionales: si es necesario, añada nombres de servidor específicos y seleccione un clúster.	No se necesita ninguna configuración.	No se necesita ninguna configuración.
Enrutar todo el tráfico a través de BlackBerry Proxy y, a continuación, a través de un servidor proxy web. Adecuada para las empresas que necesitan que todo el tráfico de las aplicaciones de trabajo se enrute internamente.	Tipo de ruta de dominio permitido por defecto: clúster de BlackBerry Proxy.	Utilice una configuración manual del servidor proxy web o un archivo PAC.	No se necesita ninguna configuración.

Situación	Perfil de conectividad de BlackBerry Dynamics	Configuración de proxy web para BlackBerry Proxy	Configuración específica de la aplicación
Enrutar parte del tráfico internamente para la mayoría de las aplicaciones, pero configurar un servidor proxy específicamente para la navegación web mediante BlackBerry Access. Adecuado para las organizaciones que requieren que el tráfico de las aplicaciones se enrute internamente, pero que necesitan que el tráfico del navegador se enrute a través de un servidor proxy web.	• Tipo de ruta de dominio permitido por defecto: directa • Dominios permitidos: añada los dominios internos que se deben enrutar a través de BlackBerry Proxy y seleccione un clúster. • Servidores adicionales: si es necesario, añada nombres de servidor específicos y seleccione un clúster.	Si los servidores BlackBerry Proxy no tienen acceso directo a Internet, o si se requiere un proxy para las conexiones BlackBerry Dynamics NOC, configure un servidor proxy web según sea necesario.	En la configuración de la aplicación para BlackBerry Access, seleccione Activar proxy web y Utilizar configuración automática de proxy.

Configuración de la autenticación de Kerberos para aplicaciones BlackBerry Dynamics

En un entorno BlackBerry UEM local, las aplicaciones BlackBerry Dynamics son compatibles con la delegación restringida Kerberos (KCD) y Kerberos PKINIT. Puede admitir KCD o Kerberos PKINIT para las aplicaciones BlackBerry Dynamics, pero no ambas.

Autenticación de Kerberos	Descripción
KCD	KCD permite a los usuarios acceder a recursos empresariales sin tener que 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 KCD, la aplicación BlackBerry Dynamics delega la autenticación a UEM para que actúe en su nombre para solicitar acceso a un recurso de trabajo. Puede limitar los recursos de red a los que pueden acceder los usuarios configurando la cuenta que utiliza UEM para que solo sea de confianza 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. Consulte Requisitos previos para configurar KCD para las aplicaciones BlackBerry Dynamics, y Configuración de KCD para aplicaciones BlackBerry Dynamics.
Kerberos PKINIT	La autenticación Kerberos PKINIT establece una confianza directa entre la aplicación BlackBerry Dynamics y el KDC Windows. La autenticación de usuario se basa en los certificados emitidos por los servicios de certificados de Microsoft Active Directory. Consulte Requisitos de compatibilidad con Kerberos PKINIT para aplicaciones BlackBerry Dynamics.

Requisitos previos para configurar KCD para las aplicaciones BlackBerry Dynamics

Elemento	Descripción
Puerto Active Directory	El puerto 88 del servicio Active Directory debe ser accesible para todos los servidores de UEM.
Entorno de Kerberos	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 de Kerberos (KCD): 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.
Nombres principales de servicio (SPN)	Cree SPN para todos los servicios HTTP, incluido BlackBerry Enterprise Mobility Server. Debe establecer un SPN para cada recurso de destino al que quiere que los dispositivos puedan acceder. Para obtener más información sobre cómo crear y modificar los SPN, consulte Registrar un nombre principal de servicio para las conexiones con Kerberos.

Elemento	Descripción
Entornos Kerberos con múltiples dominios	• Debe instalarse un UEM Core en cada dominio Kerberos como mínimo. UEM debe ubicarse en el mismo dominio Kerberos que el recurso, ya que la delegación de recursos entre dominios no es compatible. • 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. • Garantice que haya un máximo de 5 ms de latencia entre las instancias de UEM Core y la base de datos de Microsoft SQL Server.

Configuración de KCD para aplicaciones BlackBerry Dynamics

Antes de empezar:

- Revise la Requisitos previos para configurar KCD para las aplicaciones BlackBerry Dynamics.
- Si configura KCD para BlackBerry Docs, consulte Configuración de la delegación restringida Kerberos para el servicio de Docs en el contenido de BlackBerry Enterprise Mobility Server.

1. Para asignar la cuenta de servicio de Kerberos a un SPN, en el servidor Active Directory, abra el símbolo del sistema como administrador y escriba lo siguiente, especificando el nombre del servidor host, el dominio y la cuenta de servicio de Kerberos. La cuenta de servicio de Kerberos es el nombre de la cuenta de servicio bajo el que se configurará el servicio KCD en UEM (gc.krb5.principal.name). No es necesario que esta cuenta sea igual que la cuenta de servicio de UEM, pero puede serlo.

   ```
   setspn –s GCSvc/<UEM_Core_host_machine> <domain>\<Kerberos_service_account>
   ```

   Por ejemplo:

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

2. Siga estos pasos para generar un nuevo archivo keytab Kerberos y establecer la contraseña de la cuenta Kerberos:
   a) En el servidor KDC, abra una ventana del símbolo del sistema.
   b) Ejecute el siguiente comando y especifique los valores adecuados:

      ```
      ktpass -out <output_filename>.keytab -mapuser
       <Kerberos_account>@<KERBEROS_REALM_IN_ALL_CAPS> -princ
       <Kerberos_account>@<KERBEROS_REALM_IN_UPPERCASE> /ptype KRB5_NT_PRINCIPAL -
      pass <Kerberos_account_password>
      ```

   c) Copie el nuevo archivo keytab en cada servidor UEM que desee que utilice la misma cuenta de administrador de KCD.
3. Active la enumeración de miembros del grupo de objetos de usuario de Active Directory. Para obtener más información, consulte Apéndice B: Cuentas y grupos con privilegios en Active Directory.
4. En cada servidor UEM, siga estos pasos para configurar los permisos de la cuenta de servicio de UEM para que pueda enviar credenciales de usuario al sistema Kerberos (es la misma cuenta que tiene el SPN asociado):
   a) En la consola de administración Microsoft, vaya a **Política de seguridad local > Políticas locales > Asignaciones de derechos de usuario**.
   b) Abra las propiedades de **Actuar como parte del sistema operativo** y haga clic en **Añadir usuario o grupo**.
   c) Escriba el nombre de la cuenta de servicio y haga clic en **Aceptar**.

5. En la barra de menús de la consola de administración de UEM, haga clic en **Configuración > BlackBerry Dynamics > Propiedades globales**.
6. Seleccione la casilla de verificación **Utilizar UPN explícita**.
7. Seleccione la casilla de verificación **Activar KCD**.
8. Haga clic en **Guardar**.
9. En la barra de menús, haga clic en **Configuración > BlackBerry Dynamics > Propiedades** y haga clic en el nombre del servidor.
10. En el campo **Nombre completo del KDC (gc.krb5.kdc)**, escriba el nombre completo del KDC. Normalmente, se corresponde con el FQDN de un controlador de dominio de Active Directory.
11. En el campo **Ubicación del archivo keytab (gc.krb5.keytab.file)**, escriba la ubicación del archivo keytab. Utilice barras diagonales en el nombre de la ruta.
12. En el campo **Nombre de la cuenta de servicio bajo la que se ejecuta el servicio KCD (gc.krb5.principal.name)**, escriba el nombre de la cuenta de servicio utilizada por el servicio KCD.
13. En el campo **Dominio: Active Directory (gc.krb5.realm)**, escriba el nombre del dominio de Active Directory en mayúsculas.
14. Si su entorno requiere una relación de confianza CAPATH para varios dominios Kerberos, cree un archivo krb5.conf. En el campo **Ubicación del archivo krb5.config en el servidor GC (gc.krb5.config.file)**, escriba la ubicación del archivo.
15. Haga clic en **Guardar**.

Requisitos de compatibilidad con Kerberos PKINIT para aplicaciones BlackBerry Dynamics

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:

Elemento	Requisitos
KDC	• Debe añadir el host KDC a la lista de dominios permitidos en el perfil de conectividad BlackBerry Dynamics asignado. Para obtener más información, consulte Crear un perfil de conectividad de BlackBerry Dynamics en el contenido de Administración. • El host de KDC debe estar escuchando en el puerto TCP 88 (el puerto predeterminado de Kerberos). • El KDC debe tener un registro A (IPv4) o un registro AAAA (IPv6) en su DNS. • BlackBerry Dynamics no es compatible con KDC a través de UDP. • 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 añada a la lista dominios permitidos en el 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. • No se debe activar la delegación restringida Kerberos.

Elemento	Requisitos

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. • La propiedad de 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 del cliente deben incluir el nombre principal del usuario (por ejemplo, usuario@dominio.com) en el nombre alternativo del ID de objeto szOID_NT_PRINCIPAL_NAME 1.3.6.1.4.1.311.20.2.3. • Si se emite al usuario más de un certificado de cliente, el dominio del Nombre principal de usuario debe coincidir con el dominio del recurso al que se tiene acceso para garantizar que se utilice el certificado correcto. • Los certificados deben ser válidos. Valídelos en los servidores enumerados anteriormente.

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 local para que Cisco ISE pueda recuperar los datos de los dispositivos que se activan en 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 UEM. Si el dispositivo no está activado, la política de acceso puede evitar que el dispositivo se conecte a los puntos de acceso VPN o Wi-Fi de trabajo.
- Cisco ISE comprueba si el dispositivo de un usuario cumple las políticas de UEM. Si el dispositivo no cumple con las políticas (por ejemplo, el dispositivo tiene acceso a la raíz o se ha liberado), la política de acceso puede evitar que el dispositivo se conecte a los puntos de acceso VPN o Wi-Fi de trabajo.

Los administradores de Cisco ISE pueden ver, ordenar y filtrar los datos sobre los dispositivos en la consola de administración de Cisco ISE. Los administradores también pueden bloquear un dispositivo, eliminar los datos de trabajo de un dispositivo o eliminar todos los datos del dispositivo. Para obtener más información sobre el acceso a la red y los controles de dispositivos, consulte Administración del acceso a la red y de los controles del dispositivo con Cisco ISE.

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

Paso	Acción
1	Verificar que el entorno de su empresa cumple los requisitos para integrar UEM con Cisco ISE.
2	Conectar UEM a Cisco ISE y configurar un perfil de autorización y políticas de acceso.

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.

Acción	Descripción
Ver los datos del dispositivo.	Puede ver la información sobre los dispositivos asociada a BlackBerry UEM, incluida la siguiente: • Dirección MAC • Si el dispositivo es compatible con UEM • Si los datos del dispositivo están cifrados • Si el dispositivo está activado (registrado) en UEM • Si el dispositivo está descodificado o liberado • Si el dispositivo utiliza una contraseña • Fabricante • Modelo • Número de serie • Versión del SO
Configurar las 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 UEM accedan a la red de trabajo.
Bloquear un dispositivo.	Bloquee el dispositivo de un usuario. Esta característica es útil si el dispositivo de un usuario tiene una ubicación incorrecta de forma temporal. 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.
Eliminar 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. 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. 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.

Requisitos: integración de BlackBerry UEM con Cisco ISE

Elemento	Requisitos
Versión Cisco ISE	BlackBerry UEM es compatible con la integración con Cisco ISE versión 1.2 y posterior.
SO compatibles	Cualquier sistema operativo que admita UEM, excepto Windows 10 para el escritorio.
Puerto de escucha	Cisco ISE utiliza el puerto de escucha de BlackBerry Web Services predeterminado, 18084, para obtener datos sobre los dispositivos de UEM. Si el puerto 18084 no estaba disponible cuando 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 UEM y Cisco ISE, configure el firewall para permitir las sesiones HTTPS entre ambos sistemas.
Cuenta de administrador	Cisco ISE requiere una cuenta de administrador de UEM dedicada que se 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 Los roles predeterminados de administrador de seguridad y administrador de empresa tienen estos permisos, o puede crear un rol personalizado con estos permisos. Para obtener más información, consulte Creación de un administrador en el contenido de Administración.

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 UEM y la cuenta de administrador de UEM. Para obtener la documentación más reciente de Cisco ISE, visite Guías de configuración Cisco ISE.

Antes de empezar: Desde el navegador, vaya a **https://<*server_name*>:<*BlackBerry_Web_Services_port*>/enterprise/admin/util/ws?wsdl**, donde <*server_name*> es el FQDN del equipo que aloja el componente de BlackBerry UEM Core. El valor predeterminado de <*BlackBerry_Web_Services_port*> es 18084. Utilice su navegador para exportar el certificado BlackBerry Web Services y guárdelo en el escritorio.

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

2. Importe el certificado BlackBerry Web Services en el almacén de certificados de confianza de Cisco ISE. Seleccione las opciones de confianza para la autenticación de cliente y syslog, y de confianza para la autenticación de servicios Cisco.
3. Añada un servicio MDM externo y especifique los detalles de la instancia UEM, incluido el FQDN o la dirección IP del dominio UEM, el puerto (por defecto, 18084) y las credenciales de la cuenta de administrador UEM.
4. En el intervalo de sondeo, especifique con qué frecuencia (expresada en minutos) desea que Cisco ISE realice un sondeo de UEM para buscar datos del dispositivo. Se recomienda utilizar el valor predeterminado.

   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 UEM.
5. Activación y prueba de la conexión de UEM.

Una vez establecida la conexión, puede ver los atributos de diccionario de UEM en la consola de administración de Cisco ISE. 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 administración de Cisco ISE:

- Configure las ACL del controlador de LAN inalámbrica .
- Configure un perfil de autorización que redirija los dispositivos a la consola BlackBerry UEM Self-Service si intentan acceder a la red de trabajo mientras el dispositivo no está activado en UEM. El usuario requiere una cuenta de usuario de 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 UEM si Cisco ISE los redirige a la página de inscripción.
- Configure reglas de políticas de autorización que determinen cómo Cisco ISE gestiona los dispositivos que no están activados en UEM ni son compatibles con UEM.

Configuración de la VPN con Knox StrongSwan para entornos de sitio oscuro de UEM

En un entorno de sitio oscuro UEM, debe configurar el acceso VPN para su entorno para que los dispositivos Samsung Knox puedan acceder a sus servidores y recursos internos. Para obtener más información acerca de UEM en entornos de sitio oscuro, consulte Instalación o actualización de BlackBerry UEM en un entorno de sitio oscuro en el contenido de Instalación.

Antes de empezar: Descargue las aplicaciones Android VPN Management for Knox StrongSwan y Knox Service Plugin y añada los archivos .apk a la ubicación de red compartida para las aplicaciones internas.

1. Añada las aplicaciones Android VPN Management for Knox StrongSwan y Knox Service Plugin a la lista de aplicaciones.
2. Seleccione la aplicación Knox Service Plugin y haga clic en + para establecer las opciones de configuración de la aplicación.
   a) En **Perfil VPN**, seleccione **VPN integrada de Knox**.
   b) En **Parámetros para la VPN integrada de Knox para StrongSwan**, establezca las siguientes opciones:
      - Establezca el **tipo de autenticación** en "ipsec_ike2_rsa".
      - Establezca el **Alias del certificado de usuario** en el nombre de usuario con "_1 [Knox]" al final. Puede utilizar variables para el nombre de usuario (por ejemplo, `%UserFirstName% %UserLastName% _1 [Knox]`).
      - Establezca el **Alias del certificado de CA** en el nombre de usuario con "[Knox]" al final. Puede utilizar variables para el nombre de usuario (por ejemplo, `%UserFirstName% %UserLastName% [Knox]`).
3. Asigne la aplicación al usuario.
4. Cree un perfil de certificado de CA para enviar el certificado del servidor VPN a los dispositivos y asignarlo a los usuarios.
5. Añada un certificado de cliente VPN para cada usuario.

Aviso legal

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