BlackBerry UEM Cloud

Guía de configuración

Contents

Configuración de BlackBerry UEM Cloud por primera vez

La siguiente tabla muestra un resumen de las tareas de configuración incluidas en esta guía. Las tareas son opcionales en función de las necesidades de la empresa. Utilice esta tabla para determinar qué tareas de configuración se deberían completar.

Después de completar las tareas adecuadas, estará listo para configurar administradores, configurar controles de dispositivo, crear usuarios y grupos, y activar los dispositivos.

Tarea	Descripción
Conexión con el directorio local de la empresa y activación de las funciones de conectividad seguras	Puede instalar, activar y configurar BlackBerry Connectivity Node para proporcionar acceso al directorio local de la empresa y activar las funciones de conectividad seguras.
Configuración de BlackBerry Connectivity Node para enviar datos a través de un servidor proxy	Puede configurar los componentes de BlackBerry Connectivity Node para enviar datos a través de un servidor proxy en el entorno de su empresa.
Conectar BlackBerry UEM a Microsoft Azure	Si desea conectar BlackBerry UEM a Azure Active Directory, utilice BlackBerry UEM para implementar las aplicaciones iOS y Android gestionadas por Microsoft Intune o gestione las aplicaciones de Windows 10 en BlackBerry UEM y conecte BlackBerry UEM a Microsoft Azure.
Vinculación de grupos del directorio de la empresa a grupos de BlackBerry UEM	Si conecta BlackBerry UEM al directorio de la empresa, puede activar los grupos vinculados al directorio para simplificar la incorporación y gestión de usuarios.
Adquisición y registro de un certificado APN	Si desea gestionar y enviar datos a dispositivos iOS o macOS, debe obtener una CSR firmada de BlackBerry, utilizarla para obtener un certificado APN de Apple y registrar el certificado APN con el dominio de BlackBerry UEM.
ConfigureBlackBerry UEM para que admita dispositivos Android con un perfil de trabajo	Para admitir dispositivos Android que utilizan un perfil de trabajo, tiene que configurar el dominio de G Suite o de Google Cloud para que sea compatible con los proveedores de gestión de dispositivos móviles de terceros y configurar BlackBerry UEM para comunicarse con el dominio de G Suite o de Google Cloud.
Configuración de BlackBerry UEM para el programa de inscripción de dispositivos Apple	Si desea utilizar la consola de gestión de BlackBerry UEM para gestionar dispositivos iOS que su empresa adquirió de Apple para DEP, debe configurar esta función.
Configure BlackBerry UEM Cloud para admitir las aplicaciones de BlackBerry Dynamics	Si quiere permitir que los usuarios puedan utilizar aplicaciones de BlackBerry Dynamics, puede configurar BlackBerry UEM Cloud para que las admita.
Migración de usuarios, grupos y otros datos desde BlackBerry UEM	Puede utilizar la consola de administración para migrar usuarios, dispositivos, grupos y otros datos desde una base de datos local de origen de BES12 o BlackBerry UEM.

Permisos de administrador requeridos para configurar BlackBerry UEM

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

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

Adquisición y activación de licencias

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

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

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 BlackBerry UEM Cloud acceder al directorio local de la empresa. Puede crear cuentas de usuario de directorio al buscar e importar los datos del usuario desde el directorio de la empresa. Los datos del usuario se sincronizan con el directorio según la programación que configure. Si desea utilizar SCEP, BlackBerry 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. Para obtener más información, consulte Conexión de BlackBerry UEM a un conector PKI de BlackBerry Dynamics.
BlackBerry Proxy	BlackBerry Proxy mantiene una conexión segura entre su empresa y BlackBerry Dynamics NOC, permitiendo que las aplicaciones de BlackBerry Dynamics puedan comunicarse de forma segura con los recursos de su empresa detrás del 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 BlackBerry UEM Cloud para admitir las aplicaciones de 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 el contenido de administración.
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 obtener más información, consulte el contenido de administración.
BlackBerry Gatekeeping Service	BlackBerry Gatekeeping Service facilita el control de los dispositivos que pueden acceder a Exchange ActiveSync. Para obtener más información, consulte el contenido de administración.

Los archivos de instalación y de activación de BlackBerry Connectivity Node están disponibles en la consola de gestión. Puede utilizar estos archivos para instalar nuevas instancias de BlackBerry Connectivity Node y para actualizar las instancias existentes. Debe actualizar las instancias existentes de BlackBerry Connectivity Node tras implementar una nueva versión de BlackBerry UEM Cloud.

Información de planificación de BlackBerry Connectivity Node

Antes de instalar BlackBerry Connectivity Node, tenga en cuenta la siguiente información.

Hardware

BlackBerry Connectivity Node debe haberse instalado en un ordenador específico reservado para fines técnicos, en lugar de en un ordenador que se utiliza 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.

El ordenador que aloja BlackBerry Connectivity Node debe cumplir los siguientes requisitos mínimos de hardware:

- 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

Si habilita el modo de rendimiento de un solo servicio, el ordenador que aloja BlackBerry Connectivity Node debe cumplir los siguientes requisitos mínimos de hardware:

BlackBerry Connectivity Node con el modo de rendimiento de un solo servicio activado solo para BlackBerry Proxy	• 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
BlackBerry Connectivity Node con el modo de rendimiento de un solo servicio activado solo para BlackBerry Secure Connect Plus	• 4 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
BlackBerry Connectivity Node con el modo de rendimiento de un solo servicio activado solo para BlackBerry Secure Gateway	• 8 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

Software

Para verificar que su entorno cumple con los requisitos para la instalación de BlackBerry Connectivity Node, consulte la Matriz de compatibilidad.

Escalabilidad y alta disponibilidad

Cada BlackBerry Connectivity Node puede admitir hasta 5000 dispositivos. Puede instalar BlackBerry Connectivity Node s adicionales para admitir hasta 50 000 dispositivos adicionales.

Puede instalar una o más instancias de BlackBerry Connectivity Node para mejorar la redundancia. Debe instalar cada instancia en un ordenador específico. Utilice la misma configuración de directorio de la empresa para todas las instancias.

Implemente más de un BlackBerry Connectivity Node en un grupo de servidores para permitir una alta disponibilidad y equilibrio de carga.

Opcionalmente, puede designar cada BlackBerry Connectivity Node de un grupo de servidores para gestionar un único tipo de conexión: solo BlackBerry Secure Connect Plus, solo BlackBerry Secure Gateway o solo BlackBerry Proxy. Esto libera recursos del servidor para permitir que haya menos servidores requeridos 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.

Pasos para instalar y activar BlackBerry Connectivity Node

Para instalar y activar BlackBerry Connectivity Node, lleve a cabo las siguientes acciones:

1	Compruebe que su empresa cumple los requisitos previos para la instalación de BlackBerry Connectivity Node.
2	Descargue los archivos de instalación y activación de BlackBerry Connectivity Node en la consola de administración.
3	Instale, active y configure BlackBerry Connectivity Node.
4	Si es necesario, configure los ajustes de proxy de los componentes de BlackBerry Connectivity Node.
5	Realice una configuración adicional para las aplicaciones BlackBerry Secure Connect Plus, the BlackBerry Secure Gateway, the BlackBerry Gatekeeping Service, and BlackBerry Dynamics.

Requisitos previos: Instalación de BlackBerry Connectivity Node

- Verifique que el ordenador ejecuta Windows PowerShell 2.0 o posterior. Esto es necesario para que la aplicación de configuración instale el servicio RRAS para BlackBerry Secure Connect Plus y BlackBerry Gatekeeping Service.

  Nota: Si la aplicación de configuración no puede instalar el servicio RRAS en el ordenador, debe detener la instalación, instalarlo manualmente y reiniciar la instalación.
- Elija una cuenta de directorio con permisos de lectura por cada conexión de directorio configurada que BlackBerry Cloud Connector pueda usar para acceder a los directorios de la empresa.
- Utilice una cuenta de BlackBerry UEM Cloud con permisos para descargar los archivos de instalación y activación de BlackBerry Connectivity Node (por ejemplo, administrador de seguridad).
- Utilice una cuenta de Windows con permisos para instalar y configurar el software del ordenador que alojará BlackBerry Connectivity Node.
- Verifique que los siguientes puertos salientes están 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 (*región*.bbsecure.com; por ejemplo, na.region.com o eu.region.com):

- 443 (HTTPS) para activar BlackBerry Connectivity Node
- 3101 (TCP) para las demás conexiones salientes

Configuración de una variable de entorno para la ubicación de Java

BlackBerry UEM requiere que instale una implementación de JRE 8 en los servidores en los que vaya a instalar BlackBerry UEM y que tenga una variable de entorno que dirija hacia la ubicación particular de Java. Para obtener más información acerca de las versiones de JRE compatibles, consulte la Matriz de compatibilidad. Cuando comience la instalación, BlackBerry UEM verificará que pueda encontrar Java. Si ha instalado Java SE Runtime Environment de Oracle en la ubicación predeterminada, BlackBerry UEM la encontrará y configurará automáticamente la variable de entorno. Si BlackBerry UEM no puede encontrar Java, la aplicación de configuración se detendrá y deberá configurar una variable de entorno para la ubicación de Java, así como asegurarse de que la carpeta bin de Java esté incluida en la variable del sistema de la ruta.

Visite support.blackberry.com y lea el artículo 52117.

Antes de empezar: Verifique que tenga instalada una versión compatible de JDK en el servidor en el que instalará BlackBerry UEM.

1. Abra el cuadro de diálogo **Configuración avanzada del sistema de Windows**.
2. Haga clic en **Variables de entorno**.
3. En la lista **Variables del sistema**, haga clic en **Nueva**.
4. En el campo **Nombre de la variable**, escriba `BB_JAVA_HOME`.
5. En el campo **Valor de la variable**, escriba la ruta hacia la carpeta de JRE (Java Runtime Environment) y haga clic en **Aceptar**.
6. En la lista **Variables del sistema**, seleccione **Ruta** y haga clic en **Editar**.
7. Si la ruta no incluye la carpeta bin de Java, haga clic en **Nueva** y agregue `%BB_JAVA_HOME%\bin` a la ruta.
8. Mueva la entrada %BB_JAVA_HOME%\bin hacia arriba lo suficiente como para que no la pueda reemplazar ninguna otra entrada y haga clic en **Aceptar**.

Instalación o actualización de BlackBerry Connectivity Node

Siga las instrucciones de esta sección para instalar o actualizar BlackBerry Connectivity Node.

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

Debe instalar cada instancia en un ordenador específico.

Puede configurar una o más conexiones de directorio, pero si tiene varios BlackBerry Connectivity Node s, 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.

Si tiene más de un BlackBerry Connectivity Node, debe actualizar todos ellos a la misma versión de software.

Nota: Si va a actualizar varios BlackBerry Connectivity Node s, los servicios de directorio se desactivarán tras actualizar el primer nodo hasta que todos los nodos se hayan actualizado a la misma versión.

Descarga de los archivos de instalación y activación de BlackBerry Connectivity Node

1. En la barra de menús de la consola de administración, 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 el paquete de instalación.
5. 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.
6. Haga clic en **Generar**.
7. Guarde el archivo de activación (.txt).

   El archivo de activación será válido durante 60 minutos. Si espera más de 60 minutos para utilizar el archivo de activación, debe generar un nuevo archivo de activación. Solo es válido el último archivo de activación.

Después de terminar: Instalar y configurar BlackBerry Connectivity Node.

Instalar y configurar BlackBerry Connectivity Node

Antes de empezar: Descarga de los archivos de instalación y activación de BlackBerry Connectivity Node.

1. Abra el archivo de instalación (.exe) de BlackBerry Connectivity Node descargado de la consola de administración.

   Si aparece un mensaje de Windows solicitando permiso para realizar cambios en el equipo, haga clic en **Sí**.
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 (por ejemplo, na.bbsecure.com o eu.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 (por ejemplo, na.bbsecure.com o eu.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 que ha descargado de la consola de gestión.

12. Haga clic en **Activar**.

    Si desea agregar 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 (por ejemplo, na.bbsecure.com o eu.bbsecure.com) 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 la conexión**, escriba un nombre para la conexión de este directorio de empresa. **Nota:** Si tiene configurado un directorio de Microsoft Azure, este nombre de conexión debe ser diferente del nombre de la conexión del directorio Azure. **Nota:** No se puede cambiar el nombre después de guardar la configuración. **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 ordenador. 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 ordenador. 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 BlackBerry 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 la conexión**, escriba un nombre para la conexión de este directorio de empresa. **Nota:** Si tiene configurado un directorio de Microsoft Azure, este nombre de conexión debe ser diferente del nombre de la conexión del directorio Azure. **Nota:** No se puede cambiar el nombre después de guardar la configuración. **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 ordenador. 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 BlackBerry 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

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 una segunda instancia de BlackBerry Connectivity Node para mejorar la redundancia, descargue otro conjunto de archivos de instalación y activación y repita esta tarea en un ordenador diferente. Esta operación debe efectuarse tras haber activado la primera instancia.
- Puede configurar una o más conexiones de directorio, pero si tiene varios 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. Puede facilitar esta tarea Copiando configuraciones de conexiones de directorio de un BlackBerry Connectivity Node a otro.
- Si es necesario, configure los ajustes de proxy para BlackBerry Connectivity Node. Para obtener instrucciones, consulte Configuración de BlackBerry Connectivity Node para utilizar BlackBerry Router o un servidor proxy TCP.
- Para cambiar la configuración del directorio que ha configurado, en la consola de BlackBerry Connectivity Node (http:/localhost:8088), haga clic en **Configuración general > Directorio de la empresa**. Haga clic en ✎ de la conexión de directorio.
- 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 console (http://localhost:8088), haga clic en **Configuración general > Router y proxy de BlackBerry**. Active la casilla de verificación **Activar proxy HTTP** y configure los ajustes del proxy.
- 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 más información sobre la activación de BlackBerry Secure Gateway, consulte "Protección de los datos de correo electrónico con BlackBerry Secure Gateway" en el contenido de Administración.
- Para obtener instrucciones para configurar BlackBerry Gatekeeping Service, consulte "Control de los dispositivos que pueden acceder a Exchange ActiveSync" en el contenido de Configuración.

Copiar configuraciones de conexión de directorios

Si su entorno tiene varios BlackBerry Connectivity Node s, las conexiones de directorio se deben configurar de forma idéntica en todos los nodos. Para facilitar esta tarea, puede exportar la configuración de conexiones de directorio de un BlackBerry Connectivity Node e importarla a otro.

Nota: Para poder importar configuraciones del directorio de la empresa a un BlackBerry Connectivity Node, debe quitar cualquier conexión de directorio de la empresa existente de ese nodo.

1. En el BlackBerry Connectivity Node del que desee copiar la configuración, en la pantalla **Conexión del directorio de la empresa**, haga clic en **Exportar las conexiones del directorio del archivo .txt**.

   Se descargará un archivo .txt en el equipo que contiene información sobre las conexiones de directorio de la empresa.
2. En el BlackBerry Connectivity Node en el que desea copiar la configuración, en la pantalla **Conexión del directorio de la empresa**, busque el archivo .txt que ha descargado.
3. Haga clic en **Importar conexiones**.

   Las conexiones del directorio de la empresa se agregarán al BlackBerry Connectivity Node.

Cambio de la configuración predeterminada para las instancias de BlackBerry Connectivity Node

De forma predeterminada, BlackBerry Gatekeeping Service se activa en cada instancia de BlackBerry Connectivity Node. Si desea que BlackBerry Gatekeeping Service, que se ha instalado con los componentes principales de BlackBerry UEM, gestione los datos de enlace, puede cambiar el comportamiento predeterminado para desactivar BlackBerry Gatekeeping Service en cada instancia. También puede especificar la configuración predeterminada de registro para todas las instancias de BlackBerry Connectivity Node. También puede activar la configuración de BlackBerry Secure Gateway para todas las instancias de BlackBerry Connectivity Node y especificar el extremo de detección y el recurso de servidor de correo que los dispositivos iOS que ejecutan iOS 13.0 o una versión posterior deben utilizar para autenticarse en Microsoft Exchange Online con un sistema de autenticación moderno.

La configuración predeterminada se aplica a cada instancia de BlackBerry Connectivity Node que no está en un grupo de servidores. Cuando una instancia forma parte de un grupo de servidores, utiliza la configuración predeterminada configurada para dicho grupo de servidores.

1. En la barra de menús de la consola de gestión de BlackBerry UEM, haga clic en **Configuración > Integración externa > Configuración de BlackBerry Connectivity Node**.
2. Haga clic en el .
3. Si desea desactivar BlackBerry Gatekeeping Service en cada instancia, seleccione la casilla de verificación **Anular configuración de BlackBerry Gatekeeping Service**.
4. Si desea configurar la configuración de registro, seleccione la casilla de verificación **Anular configuración de registro**. Lleve a cabo cualquiera de las tareas 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 especificar límites máximos del tamaño y la antigüedad del archivo de registro, seleccione la casilla de verificación **Activar destino de archivo local**. Especifique el límite de tamaño (en MB) y el límite de antigüedad (en días).
5. Si desea especificar BlackBerry Secure Gateway en cada instancia, seleccione la casilla de verificación **Anular configuración de BlackBerry Secure Gateway**. Para dispositivos iOS que ejecutan 13.0 o posterior y utilizan un sistema de autenticación moderno para conectarse a Microsoft Exchange Online, realice los siguientes pasos para especificar el extremo de detección y el recurso de servidor de correo:
   a) Seleccione la casilla de verificación **Activar OAuth para la autenticación del servidor de correo**.
   b) En el campo **Extremo de detección**, especifique la dirección URL que se utilizará para las solicitudes de detección que utilizan OAuth. Introduzca el extremo de detección con el formato https://*proveedor de identidades*>/.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 e identificaciones mediante Oauth (por ejemplo, `https://outlook.office365.com`).
6. Haga clic en **Guardar**.

Después de terminar: Si desactiva las instancias de BlackBerry Gatekeeping Service y desea activarlas de nuevo, seleccione la casilla de verificación **Activar BlackBerry Gatekeeping Service**. Cada instancia debe poder acceder al servidor de enlace de su empresa.

Actualizar BlackBerry Connectivity Node

Cuando se le notifique que hay una actualización para BlackBerry UEM Cloud, siga las siguientes instrucciones para actualizar los componentes de BlackBerry Connectivity Node a la última versión.

1. En el ordenador que aloja BlackBerry Connectivity Node, abra la consola de BlackBerry Connectivity Node (http:/localhost:8088).
2. Registre los ajustes de la configuración del directorio actual.
3. Inicie sesión en la consola de gestión de BlackBerry UEM Cloud.
4. Descargue los archivos de instalación y activación de BlackBerry Connectivity Node. Para obtener instrucciones, consulte Descarga de los archivos de instalación y activación de BlackBerry Connectivity Node.
5. Instale y configure BlackBerry Cloud Connector utilizando la información que haya registrado en el paso 2. Para obtener instrucciones, consulte Instalar y configurar BlackBerry Connectivity Node.

Creación de grupos de servidores

Puede configurar las conexiones regionales para funciones de conectividad de la empresa mediante la implementación de una o más instancias de BlackBerry Connectivity Node en una región específica. Esto se conoce 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. Puede asociar perfiles de correo y de conectividad de empresa con un grupo de servidores. Cualquier dispositivo que se asigne a estos perfiles usa la conexión regional del grupo de servidores a BlackBerry Infrastructure cuando utiliza cualquiera de los componentes de BlackBerry Connectivity Node.

La implementación de uno o más BlackBerry Connectivity Node en un grupo de servidores también permite una alta disponibilidad y equilibrio de carga.

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

Creación de un grupo de servidores

Antes de empezar: Instale BlackBerry Connectivity Node adicional

1. En la barra de menús, 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 donde se instalarán una o más instancias de BlackBerry Connectivity Node. Las instancias de BlackBerry Connectivity Node que se agregan al grupo de servidores utilizarán la conexión regional del país seleccionado con BlackBerry Infrastructure.

   Nota: No puede cambiar este ajuste después de crear el grupo de servidores.
5. De forma predeterminada, cada instancia de BlackBerry Connectivity Node debe configurarse para el mismo directorio de empresa. Si desea desactivar el conector del directorio de empresa para las instancias de BlackBerry Connectivity Node en el grupo de servidores, seleccione la casilla para marcar **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 que hay establecida en **Configuración > Infraestructura > BlackBerry Secure Connect Plus**, seleccione la casilla para marcar **Anular servidores DNS**. Realice las tareas siguientes:
   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.

Para obtener más información, consulte "Activación y configuración de la conectividad de empresa de BlackBerry Secure Connect Plus" en el contenido de Administración.

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**. Lleve a cabo cualquiera de las tareas 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 especificar límites máximos del tamaño y la antigüedad del archivo de registro, seleccione la casilla de verificación **Activar destino de archivo local**. Especifique el límite de tamaño (en MB) y el límite de antigüedad (en días).
9. Si desea designar el BlackBerry Connectivity Node solo para un tipo de conexión, seleccione la casilla de verificación **Activar modo de rendimiento de servicio único**. En el menú desplegable, seleccione el tipo de conexión (**Solo BlackBerry Secure Connect Plus**, **Solo BlackBerry Secure Gateway** o **Solo BlackBerry Proxy**).
10. Si desea especificar los ajustes de BlackBerry Secure Gateway para la instancia BlackBerry Connectivity Node en el grupo de servidores, seleccione la casilla de verificación **Configuración de BlackBerry Secure Gateway**. Para dispositivos con iOS que ejecutan iOS 13.0 o posterior, que utilizan un sistema de autenticación moderno para conectarse a Microsoft Exchange Online, especifique el extremo de detección y el recurso de servidor de correo.
    a) Seleccione la casilla de verificación **Activar OAuth para la autenticación del servidor de correo**.
    b) En el campo **Extremo de detección**, especifique la dirección URL que se utilizará para las solicitudes de detección que utilizan OAuth para la autenticación. Introduzca el extremo de detección con el formato https://*proveedor de identidades*>/.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:

- Si ha desactivado las instancias de BlackBerry Gatekeeping Service en un grupo de servidores y desea activarlas de nuevo, en **Configuración > Integración externa > Configuración de BlackBerry Connectivity Node**, seleccione el grupo de servidores y la casilla de verificación **Activar BlackBerry Gatekeeping Service**. Cada instancia debe poder acceder al servidor de enlace de su empresa.
- Instalar y configurar BlackBerry Connectivity Node y agregar la instancia a un grupo de servidores.

Gestión de grupos de servidores

Puede agregar una instancia de BlackBerry Connectivity Node a un grupo de servidores o eliminar una instancia de un grupo de servidores en cualquier momento. Si agrega una instancia a un grupo de servidores, la instancia utiliza la configuración que ha configurado para dicho grupo de servidores (por ejemplo, los componentes de esa instancia utilizarán la conexión regional especificada de BlackBerry Infrastructure). Si elimina una instancia de un grupo de servidores, dicha instancia utiliza la configuración predeterminada que se ha configurado en la pantalla de configuración de BlackBerry Connectivity Node (consulte Cambio de la configuración predeterminada para las instancias de BlackBerry Connectivity Node).

1. En la barra de menú de la consola de gestión de BlackBerry UEM, haga clic en **Configuración > Integración externa > Configuración de BlackBerry Connectivity Node**.
2. Seleccione una instancia de BlackBerry Connectivity Node.
3. Lleve a cabo una de las tareas siguientes:
   a) Para agregar una instancia a un grupo de servidores, haga clic en . Seleccione el grupo de servidores correspondiente. Haga clic en **Aceptar**.
   b) Para eliminar una instancia de un grupo de servidores, haga clic en . En el cuadro de diálogo de confirmación, haga clic en **Aceptar**.

Resolución de problemas de BlackBerry Connectivity Node

A la hora de solucionar problemas con BlackBerry Connectivity Node, tenga en cuenta los inconvenientes más comunes que se mencionan a continuación.

Para obtener más información sobre los recursos de soporte de BlackBerry, visite el servicio de soporte técnico de BlackBerry.

BlackBerry Connectivity Node no se activa con BlackBerry UEM Cloud

Descripción

Después de cargar el archivo de activación y hacer clic en Activar, recibirá un mensaje de error que indica que la activación no se ha realizado correctamente.

Posibles soluciones

Intente realizar alguna de las siguientes acciones:

- 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.
- Los archivos de activación caducan después de 60 minutos. Genere y cargue un nuevo archivo de activación y, a continuación, intente realizar de nuevo la activación.
- Visite support.blackberry.com/community para leer el artículo 38964.

BlackBerry Connectivity Node no establece conexión con el directorio de la empresa

Descripción

Después de especificar la información del directorio de la empresa y hacer clic en Guardar, recibirá un mensaje de error que indica que BlackBerry Connectivity Node no puede establecer conexión con el directorio de la empresa.

Posibles soluciones

Intente realizar alguna de las siguientes acciones:

- Si tiene varios BlackBerry Connectivity Node s, compruebe que todos tienen la misma versión de software.
- Compruebe que ha especificado la configuración correcta para el directorio de la empresa.
- Compruebe que todos los BlackBerry Connectivity Node s tienen una conexión de directorio y que las conexiones de directorio están configuradas de forma idéntica en todos los BlackBerry Connectivity Node s inscritos.

- 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 de BlackBerry Connectivity Node se ubican en *<unidad:>*:\Archivos de programa\BlackBerry \BlackBerry Connectivity Node\Logs.
- Si está utilizando Microsoft Active Directory, visite support.blackberry.com/community y lea el artículo 36955.

BlackBerry Connectivity Node no establece conexión con BlackBerry UEM Cloud

Descripción

Al probar la conexión entre BlackBerry Connectivity Node y BlackBerry UEM Cloud, recibirá un mensaje de error que indica que la prueba no se ha realizado correctamente.

Posibles soluciones

Intente realizar alguna de las siguientes acciones:

- Verifique que los siguientes puertos salientes están 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 (*región*.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 BlackBerry UEM Cloud. De forma predeterminada, los archivos de registro de BlackBerry Cloud Connector se ubican en *<unidad:>*:\Archivos de programa\BlackBerry \BlackBerry Connectivity Node\Logs.

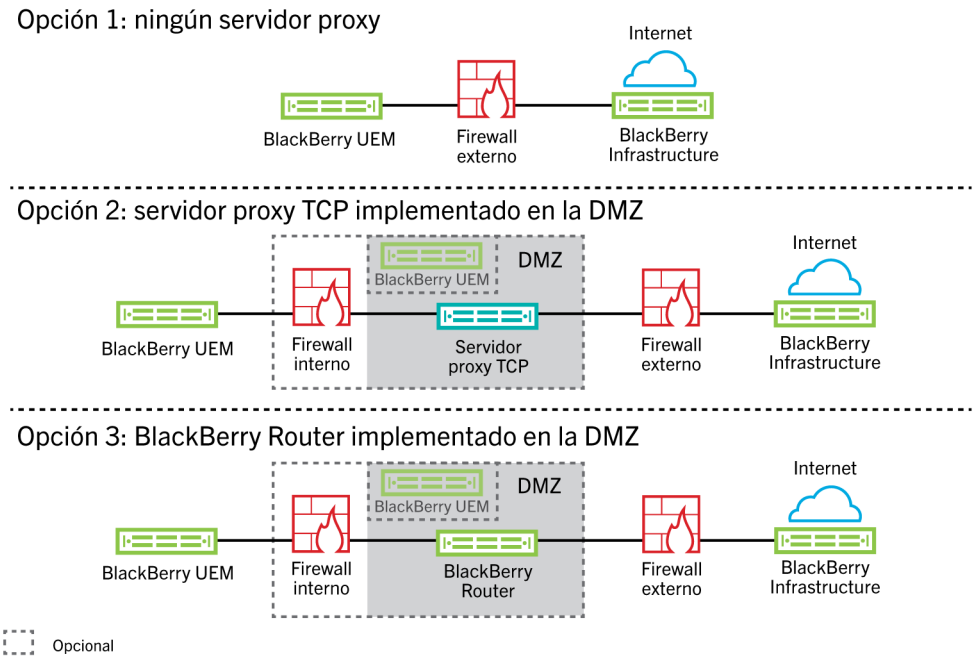
Configuración de BlackBerry Connectivity Node para utilizar BlackBerry Router o un servidor proxy TCP

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. No obstante, 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.

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



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

Al activar BlackBerry Connectivity Node, se envían los datos a través del puerto 443 (HTTPS) para la activación con BlackBerry UEM Cloud. 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 BlackBerry UEM. Varios servidores proxy TCP configurados con SOCKS v5 (sin autenticación) pueden proporcionar apoyo si una de las instancias de servidor proxy activo no está funcionando correctamente.

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

Comparación de los servidores proxy TCP

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

Configuración de BlackBerry UEM para utilizar un servidor proxy TCP transparente

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

1. En la consola de BlackBerry Connectivity Node (http:/localhost:8088), haga clic en **Configuración general > Proxy**.
2. Seleccione la opción **Servidor proxy**.
3. Lleve a cabo cualquiera de las tareas siguientes:

Tarea	Pasos
Enrute los datos de activación HTTPS para BlackBerry Connectivity Node a través de un servidor proxy.	En los campos **Proxy de inscripción**, introduzca 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 <*región*>.bbsecure.com.
Enrute las conexiones salientes de 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 <*región*>.bbsecure.com.

4. Haga clic en **Guardar**.

Activación de SOCKS v5 en un servidor proxy TCP

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

1. En la consola de BlackBerry Connectivity Node (http:/localhost:8088), haga clic en **Configuración general > Proxy**.
2. Seleccione la opción **Servidor proxy**.
3. Seleccione la casilla de verificación **Activar SOCKS v5**.
4. Haga clic en +.
5. En el campo **Dirección del servidor**, escriba la dirección IP o el nombre de host del servidor proxy SOCKS v5.
6. Haga clic en **Agregar**.
7. Repita los pasos 1 a 6 para cada servidor proxy SOCKS v5 que desea configurar.
8. En el campo **Puerto**, escriba el número de puerto.
9. Haga clic en **Guardar**.

Instalación de BlackBerry Router independiente

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).

Nota: Si su entorno actual contiene un servidor proxy TCP, no necesita instalar BlackBerry Router.

Instalación de un BlackBerry Router independiente

Antes de empezar:

- Debe instalar un BlackBerry Router independiente en un ordenador que no aloje ningún otro componente de BlackBerry UEM. No puede instalar BlackBerry Router en un ordenador que aloje BlackBerry Connectivity Node.
- Compruebe que dispone del nombre del host de SRP. Por lo general, el nombre del host de SRP es <*código de país*>.srp.blackberry.com (por ejemplo, *us*.srp.blackberry.com). Para comprobar el nombre de host de SRP de su país, visite la página Búsquedas de direcciones SRP.

1. En la barra de menús de la consola de gestión, haga clic en **Configuración > Integración externa > BlackBerry Cloud Connector**.
2. Haga clic en **Agregar BlackBerry Connectivity Node**.
3. En el **paso 1: en la sección Descargar BlackBerry Connectivity Node**, 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. Haga doble clic en el archivo **Setup.exe**.

   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.

Envío de datos a través de BlackBerry Router a BlackBerry Infrastructure

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

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.

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

Configuración de BlackBerry UEM para utilizar BlackBerry Router

Antes de empezar: Instalación de un BlackBerry Router independiente.

1. En la consola de BlackBerry Connectivity Node (http:/localhost:8088), haga clic en **Configuración general > Proxy**.
2. Seleccione la opción **BlackBerry Router**.
3. Haga clic en +.
4. Escriba la dirección IP o el nombre de host de la instancia de BlackBerry Router que desee conectar a BlackBerry UEM.
5. Haga clic en **Agregar**.
6. Repita los pasos 1 a 5 para cada instancia de BlackBerry Router que desee configurar.
7. En el campo **Puerto**, escriba el número de puerto que todas las instancias de BlackBerry Router escuchan. El valor predeterminado es 3102.
8. Haga clic en **Guardar**.

Conexión de BlackBerry UEM a Microsoft Azure

Microsoft Azure es el servicio informático en la nube de Microsoft para la implementación y la gestión de aplicaciones y servicios. La conexión de BlackBerry UEM a Azure ofrece a su empresa las siguientes funciones:

- Conectar BlackBerry UEM a Azure Active Directory y crear cuentas de usuario de directorio en BlackBerry UEM buscando e importando los datos del usuario desde el directorio de la 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.
- Utilice BlackBerry UEM para implementar las aplicaciones iOS y Android gestionadas por Microsoft Intune.
- gestionar aplicaciones de Windows 10 en BlackBerry UEM

Si su empresa utiliza Microsoft Active Directory en lugar de Azure Active Directory, para conectarse a Azure, debe instalar la versión más reciente de BlackBerry Connectivity Node para que BlackBerry UEM Cloud pueda acceder al directorio de la empresa.

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

Paso	Acción
1	Crea una cuenta de Microsoft Azure.
2	Si su empresa utiliza Azure Active Directory, configure BlackBerry UEM Cloud para que se sincronice con Azure Active Directory.
3	Si su empresa utiliza una versión local de Microsoft Active Directory y desea utilizar BlackBerry UEM para implementar aplicaciones gestionadas por Microsoft Intune o gestionar aplicaciones de Windows 10, Sincronización de Microsoft Active Directory con Microsoft Azure.
4	Cree aplicaciones empresariales en Azure para que BlackBerry UEM Cloud pueda conectarse a Microsoft Intune y la Windows Store para empresas.
5	Configure BlackBerry UEM para que se sincronice con Microsoft Intune y Windows Store for Business.
6	(Opcional) Configure el acceso condicional de Azure Active Directory.

Crea una cuenta de Microsoft Azure

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

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

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

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

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

Configuración de BlackBerry UEM para que se sincronice con Azure Active Directory

Si su empresa utiliza Microsoft Azure Active Directory, puede conectarlo a BlackBerry UEM para crear cuentas de usuario del directorio en BlackBerry UEM buscando e importando los datos de usuario desde el directorio de la empresa. Los usuarios de directorio pueden utilizar las credenciales para acceder a BlackBerry UEM Self-Service.

Puede realizar la conexión a más de una instancia de Azure Active Directory. Si instala BlackBerry Connectivity Node, también puede realizar la conexión a un directorio local.

1. Inicie sesión en el portal de Azure.
2. Vaya a **Microsoft Azure > Azure Active Directory > Registros de aplicaciones**.
3. Haga clic en **+ Nuevo registro**.
4. En el campo **Nombre**, escriba un nombre para la aplicación.
5. Seleccione los tipos de cuenta que usarán la aplicación o accederán a la API.
6. En la sección **URI de redirección**, en la lista desplegable, seleccione **Web** e introduzca `http://localhost`.
7. Haga clic en **Registrar**.
8. Copie el **ID de aplicación** de su aplicación y péguelo en un archivo de texto.

   Este es el **ID de cliente** que se requiere en BlackBerry UEM.
9. En la sección **gestionar**, haga clic en **Permisos de API**.
10. Haga clic en **+ Agregar un permiso** y realice las siguientes acciones:
    a) Haga clic en **Microsoft Graph**.
    b) Seleccione **Permisos de aplicaciones**.
    c) Configure los siguientes permisos:
       - Group.Read.All (aplicación)
       - User.Read (delegado)
       - User.Read.All (aplicación)
    d) Haga clic en **Agregar permiso**.
    e) En **Conceder permiso**, haga clic en **Conceder permiso de admin.**.

       Nota: Debe ser un administrador global para conceder los permisos.
    f) Cuando se le solicite, haga clic en **Sí** para conceder permisos para todas las cuentas en el directorio actual.
11. En la sección **Gestión**, haga clic en **Certificados y secretos**. Realice las acciones siguientes:
    a) En **Secretos de cliente**, haga clic en **Nuevo secreto de cliente**.
    b) Escriba una descripción para el secreto de cliente.
    c) Seleccione una duración para el secreto de cliente.
    d) Haga clic en **Agregar**.
    e) Copie el valor del nuevo secreto de cliente.

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

12. En la consola de administración, haga clic en **Configuración > Integración externa > + Directorio de la empresa > Conexión de Microsoft Azure Active Directory**.
13. Introduzca el **Nombre de la conexión de directorio** y el **Dominio** de su Azure Active Directory.
14. Lleve a cabo una de estas acciones:
    - Si se trata de una nueva conexión a Azure, introduzca la información que copió del portal de Azure cuando creó la aplicación empresarial en Azure.
      - **ID de cliente**: el ID de aplicación generado por el registro de aplicación Azure
      - **Clave de cliente**: la clave de cliente generada por el registro de aplicación Azure
    - Si se trata de una conexión existente a Azure, haga clic en **Activar registro de aplicaciones de único inquilino** e introduzca la información que copió del portal de Azure cuando creó la aplicación empresarial en Azure.
      - **ID de cliente**: el ID de aplicación generado por el registro de aplicación Azure
      - **Clave de cliente**: la clave de cliente generada por el registro de aplicación Azure
15. Haga clic en **Continuar**.
16. Haga clic en **Guardar**.

Después de terminar: Vinculación de grupos del directorio de la empresa a grupos de BlackBerry UEM

Sincronización de Microsoft Active Directory con Microsoft Azure

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

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

Después de terminar: Creación de un extremo empresarial en Azure

Creación de un extremo empresarial en Azure

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

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

Nota:

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

Antes de empezar:

- Si su empresa utiliza una versión local de Microsoft Active Directory: Sincronización de Microsoft Active Directory con Microsoft Azure
- Asegúrese de tener una URL de respuesta. Para obtener más información sobre cómo obtener la URL de respuesta para las autenticaciones modernas, consulte Configurar BlackBerry UEM para su sincronización con Microsoft Intune.

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

   Este es el **ID de cliente** que se requiere en BlackBerry UEM.
9. Si va a crear la aplicación para utilizar Microsoft Intune, haga clic en **Permisos de API** en la sección **Administrar**. Realice los siguientes pasos:
   a) Haga clic en **Agregar un permiso**.
   b) Haga clic en **Microsoft Graph**.
   c) Seleccione **Permisos delegados**.
   d) Desplácese hacia abajo por la lista de permisos y en **Permisos delegados** establezca los siguientes permisos para Microsoft Intune:
      - Lea y escriba aplicaciones de Microsoft Intune (**DeviceManagementApps > DeviceManagementApps.ReadWrite.All**)
      - Lea todos los grupos (**Group > Group.Read.All**)
      - Lea el perfil básico de todos los usuarios (**User > User.ReadBasic.All**)
   e) Haga clic en **Agregar permisos**.
   f) En **Conceder consentimiento**, haga clic en **Conceder consentimiento de administrador**.

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

   Puede utilizar los permisos predeterminados si va a crear la aplicación para que se conecte a Windows Store for Business.
10. Haga clic en **Certificados y secretos** en la sección **Administrar**. Realice las acciones siguientes:
    a) En **Secretos de cliente**, haga clic en **Nuevo secreto de cliente**.
    b) Escriba una descripción para el secreto de cliente.
    c) Seleccione una duración para el secreto de cliente.
    d) Haga clic en **Agregar**.
    e) Copie el valor del nuevo secreto de cliente.

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

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

Después de terminar: Configurar BlackBerry UEM para su sincronización con Microsoft Intune

o Configurar BlackBerry UEM para su sincronización con la Tienda Windows para empresas.

Configuración del acceso condicional de Azure Active Directory

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

Puede configurar conexiones a varios inquilinos de Azure. Si crea varias conexiones:

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

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

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

- Los usuarios deben existir en Azure AD,
- Si está sincronizando su Active Directory local a Azure AD, la UPN de Active Directory local de los usuarios debe coincidir con su UPN de Azure AD. Si estos valores no coinciden en su entorno, visite support.blackberry.com/community para leer el artículo 88208.
- Los usuarios deben agregarse UEM a aunque se sincronice con Active Directory.
- Los usuarios deben tener la aplicación Authenticator Microsoft instalada y BlackBerry UEM Client instalada.

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

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

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

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

Configurar BlackBerry UEM como socio de cumplimiento en Azure

Antes de empezar: Debe utilizar la licencia de Microsoft Intune adecuada para usar esta función. Para obtener más información, visite support.blackberry.com y lea los artículos KB91041 y KB50341. Para obtener más información sobre las licencias, consulte los detalles de Microsoft. La cuenta de administrador que utilice para completar los siguientes pasos debe tener una licencia de Intune.

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

Si es compatible con dispositivos con iOS y Android, debe agregar BlackBerry UEM como socio de cumplimiento para cada plataforma. Para obtener más información, consulte la documentación de Microsoft.

Configuración de acceso condicional de Azure Active Directory.

1. En la consola de administración de BlackBerry UEM, haga clic en **Configuración > Integración externa > Acceso condicional de Azure Active Directory**.
2. En la tabla, haga clic en +.
3. Escriba un nombre para la configuración.
4. En la lista desplegable **Azure Cloud**, seleccione **Global**.
5. Introduzca su **ID de inquilino de Azure**.

   Puede introducir el nombre del grupo de usuarios, que está en formato FQDN, o el ID único del grupo de usuarios, que está en formato GUID.
6. En la anulación de asignación de dispositivos, seleccione **UPN** o **Correo electrónico**.

   UPN está seleccionado de forma predeterminada. Si se utiliza UPN, debe comprobar que el inquilino de Azure AD y todos los directorios asignados comparten el mismo valor de UPN para los usuarios antes de guardar la conexión. Después de guardar la conexión, la anulación de asignación de dispositivos no se puede cambiar.
7. En la lista **directorios disponibles de la empresa**, seleccione una o más instancias de directorio y haga clic en ➡.
8. Haga clic en **Guardar**.
9. Seleccione la cuenta de administrador que desea utilizar para iniciar sesión en su Azure inquilino.

   La cuenta de administrador debe ser capaz de otorgar permisos a la aplicación para acceder a los recursos de su empresa. como el administrador global, el administrador de aplicaciones en la nube o el administrador de aplicaciones.
10. Acepte la solicitud de permiso de Microsoft.

Configure el perfil de conectividad de BlackBerry Dynamics para que sea compatible con la función de acceso condicional de Azure

En la consola de administración de BlackBerry UEM, edite cada perfil de conectividad de BlackBerry Dynamics.

1. En Servidores de aplicaciones, haga clic en Agregar.
2. Seleccione **Función-Acceso condicional de Azure** en la lista de aplicaciones.
3. Haga clic + para agregar un nuevo servidor de aplicaciones.
4. Si está utilizando BlackBerry UEM en un entorno local, especifique la siguiente configuración del servidor:

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

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

Asigne la aplicación Función-Acceso condicional de Azure a usuarios

Puede asignar la aplicación a usuarios o a grupos.

Lleve a cabo una de estas acciones:

Tarea	Pasos
Asignar la aplicación a un usuario	**a.** En la barra de menús, haga clic en **Usuarios > Dispositivos gestionados**. **b.** En los resultados de la búsqueda, haga clic en el nombre de una cuenta de usuario. **c.** En la sección **Aplicaciones**, haga clic en **+**. **d.** Busque y seleccione la aplicación Función-Acceso condicional a Azure. **e.** Haga clic en **Siguiente**. **f.** Si lo prefiere, complete los campos **Disposición**, **VPN por aplicación** y **Configuración de la aplicación**. **g.** Haga clic en **Asignar**.
Asignar la aplicación a un grupo	**a.** En la barra de menús, haga clic en **Grupos**. **b.** En la pestaña **Grupos de usuario**, haga clic en el nombre de un grupo. **c.** En la sección **Aplicaciones asignadas**, haga clic en **+**. **d.** Busque y seleccione la aplicación Función-Acceso condicional a Azure. **e.** Haga clic en **Siguiente**. **f.** Si lo prefiere, complete los campos **Disposición**, **VPN por aplicación** y **Configuración de la aplicación**. **g.** Haga clic en **Asignar**.

Configurar un perfil de BlackBerry Dynamics

1. En la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Política > BlackBerry Dynamics**.
3. Haga clic en **+**.
4. Escriba un nombre y una descripción para el perfil.
5. Seleccione la opción **Activar UEM Client para que pueda inscribirse en BlackBerry Dynamics**.
6. Configure los valores adecuados para el resto de la configuración del perfil. Para obtener más información acerca de cada configuración de perfil, consulte Configuración del perfil de BlackBerry Dynamics.
7. Haga clic en **Agregar**.

Después de terminar:

- La aplicación Microsoft Authenticator debe estar instalada en los dispositivos de los usuarios. Puede descargar la aplicación en la tienda de aplicaciones correspondiente y agregarla a UEM. Para obtener más información, consulte la información de iOS y la información de Android. Puede asignar la aplicación a usuarios o a grupos. También puede indicar a los usuarios que la instalen desde su tienda de aplicaciones.
- Después de configurar el acceso condicional de Active Directory, se solicita a los usuarios que activen los dispositivos que se registren con acceso condicional de Active Directory durante la activación. Se solicita a los usuarios con dispositivos activados que se registren con acceso condicional de Active Directory la siguiente vez que abran UEM Client.

Quitar dispositivos del acceso condicional de Azure Active Directory

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

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

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

Vinculación de grupos del directorio de la empresa a grupos de BlackBerry UEM

Puede crear grupos en BlackBerry UEM que estén vinculados a los grupos del directorio de la empresa. Al activar los grupos vinculados a directorios, puede aprovechar las siguientes características:

- Capacidad para agregar grupos en BlackBerry UEM que están vinculados a los grupos del directorio de la empresa con el propósito de asignar y gestionar las políticas, los perfiles y las aplicaciones de TI para los usuarios. Estos grupos se denominan grupos vinculados a directorios.

  Para obtener más información acerca de la creación de grupos vinculados al directorio, consulte el contenido referente a Administración.
- Capacidad para agregar grupos en BlackBerry UEM que están vinculados a los grupos del directorio de la empresa con el propósito de sincronizar automáticamente los miembros del grupo. Estos grupos se denominan grupos de directorio de integración. Consulte Permitir integración.

Permitir los grupos vinculados al directorio

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

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

   Si se selecciona, cuando un grupo se elimina del directorio de su empresa, los vínculos a ese grupo se eliminan de grupos vinculados a directorios y grupos de directorio de integración. Si todos los grupos de directorios de la empresa asociados a un grupo vinculado a directorios se eliminan, el grupo vinculado a directorios se convertirá en un grupo local. Si no se seleccionan, en caso de no encontrar un grupo de directorios de la empresa, el proceso de sincronización se cancela.
5. En el campo **Límite de sincronización**, escriba el número máximo de cambios que desea permitir para cada proceso de sincronización.

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

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

Permitir integración

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

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

Extracción

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

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

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

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

Sincronización

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

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

Activación y configuración de la integración y la extracción

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

Antes de empezar:

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

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

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

    La protección de la extracción implica que los usuarios no se borrarán de BlackBerry UEM hasta dos horas después del siguiente ciclo de sincronización.
11. Para forzar la sincronización de los grupos de directorios de la empresa, seleccione la casilla de verificación **Forzar sincronización**.

    Si se selecciona, cuando un grupo se elimina del directorio de la empresa, los vínculos a ese grupo se eliminan de los grupos de directorios de integración y los grupos vinculados a directorios. Si no se selecciona, en caso de no encontrar un grupo de directorios de la empresa, el proceso de sincronización se cancela.
12. En el campo **Límite de sincronización**, escriba el número máximo de cambios que desea permitir para cada proceso de sincronización. La configuración predeterminada es cinco.

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

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

Sincronización de una conexión de directorio de empresa

Antes de empezar: Vista previa del informe de sincronización

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

Después de terminar: Visualización de un informe de sincronización

Vista previa del informe de sincronización

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

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

Visualización de un informe de sincronización

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

Agregar un programa de sincronización

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

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

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

1. En la barra de menús, haga clic en **Configuración > Integración externa > Directorio de la empresa**.
2. Haga clic en el nombre del directorio de la empresa que desea editar.
3. En la pestaña **Programación de sincronización**, haga clic en +.
4. Para reducir la cantidad de información que se sincroniza, en la lista desplegable **Tipo de sincronización**, elija una de las siguientes opciones:
   - **Todos los grupos y usuarios**: Esta es la configuración predeterminada. Si selecciona esta opción, los usuarios se integrarán, extraerán y vincularán a los grupos vinculados del directorio pertinente durante la

sincronización. Se sincronizarán los usuarios que no se integren ni extraigan, pero que cambien de grupos vinculados a directorios, y aquellos con cambios en sus atributos.

- **Incorporación de grupos**: Si selecciona esta opción, los usuarios se incorporarán, eliminará y vincularán a los grupos vinculados del directorio pertinente durante la sincronización y se sincronizarán aquellos usuarios con cambios en sus atributos. Los usuarios que no se integren ni se extraigan, pero que cambien de grupos vinculados a directorios no se vincularán.
- **Grupos vinculados a directorios**: Si elige esta opción, los usuarios no podrán incorporarse ni eliminarse durante la sincronización. Los usuarios con cambios en sus grupos vinculados a directorios se vincularán adecuadamente. Los usuarios con cambios en sus atributos se sincronizarán.
- **Atributos de usuario**: Si elige esta opción, los usuarios no podrán incorporarse ni eliminarse durante la sincronización. Los usuarios con cambios en sus grupos vinculados a directorios no se sincronizarán. Los usuarios con cambios en sus atributos se sincronizarán.

5. En la lista desplegable **Repetición**, seleccione una de las opciones siguientes:

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

6. Haga clic en **Agregar**.

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.

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

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

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

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

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

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

Obtener una CSR firmada de BlackBerry

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

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

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

Después de terminar: Solicitar un certificado APN de Apple.

Solicitar un certificado APN de Apple

Antes de empezar: Obtener una CSR firmada de BlackBerry.

1. En la barra de menú, haga clic en **Configuración > Integración externa > Apple Push Notification**.
2. En la sección **Paso 2 de 3: Solicitar un certificado APN de Apple**, haga clic en **Portal de certificados de inserción de Apple**. Se le dirige al portal de certificados de inserción de Apple.
3. Inicie sesión en el portal de certificados de inserción de Apple a través de un ID de Apple válido.
4. Siga las instrucciones para cargar la CSR firmada (.scsr). Tenga en cuenta que, si aparece el siguiente error: "Ha cargado un tipo de archivo no válido. Las extensiones de archivo compatibles son .txt, .rtf, .plist, .b64", puede cambiar el nombre del archivo .scsr a un formato de archivo .txt y cargar la CSR de nuevo.
5. Descargue y guarde el certificado APN (.pem) en el equipo.
6. (Opcional) Haga clic en para mostrar la ventana **Nota**.
7. En la ventana **Nota**, escriba el ID de Apple que utilizó para solicitar el certificado APN.

   Debe utilizar el mismo ID de Apple para renovar el certificado.
8. Haga clic en cualquier sitio fuera de la ventana **Nota** para cerrarla.

Después de terminar: Registro del certificado APN.

Registro del certificado APN

Antes de empezar: Solicitar un certificado APN de Apple.

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

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

Renovación del certificado APN

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

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

Antes de empezar: Obtener una CSR firmada de BlackBerry.

1. En la barra de menú, haga clic en **Configuración > Integración externa > Apple Push Notification**.
2. Haga clic en **Renovar certificado**.
3. En la sección **Paso 1 de 3: Descargar el certificado CSR firmado de BlackBerry**, haga clic en **Descargar certificado**.
4. Haga clic en **Guardar** para guardar el archivo CSR firmado (.scsr) en el equipo.
5. En la sección **Paso 2 de 3: Solicitar un certificado APN de Apple**, haga clic en **Portal de certificados de inserción de Apple**. Se le dirige al portal de certificados de inserción de Apple.

6. Inicie sesión en el portal de certificados de inserción de Apple a través del mismo ID de Apple que utilizó para obtener el certificado APN original.
7. Siga las instrucciones para renovar el certificado APN (.pem). Tendrá que cargar la nueva CSR firmada. Tenga en cuenta que, si aparece el siguiente error: "Ha cargado un tipo de archivo no válido. Las extensiones de archivo compatibles son .txt, .rtf, .plist, .b64", puede cambiar el nombre del archivo .scsr a un formato de archivo .txt y cargar la CSR de nuevo.
8. Descargue y guarde el certificado APN renovado en el equipo.
9. En la sección **Paso 3 de 3: Registrar el certificado APN**, haga clic en **Examinar**. Vaya al certificado APN renovado y selecciónelo.
10. Haga clic en **Submit**.

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

Solución de problemas de APN

Esta sección le ayuda a solucionar problemas de APN.

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

Descripción

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

Solución posible

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

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

Descripción

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

Solución posible

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

No puedo activar dispositivos con iOS o macOS

Causa posible

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

Solución posible

Realice una o más de las acciones siguientes:

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

Configuración de BlackBerry UEM para DEP

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

Puede utilizar una cuenta de Apple Business Manager para sincronizar BlackBerry UEM con DEP. Apple Business Manager es un portal basado en web en el que puede inscribir y gestionar dispositivos iOS en DEP, así como gestionar cuentas VPP de Apple. Si su empresa utiliza DEP o VPP, puede actualizar a Apple Business Manager.

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

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

Creación de una cuenta de DEP

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

Después de terminar: Descarga de una clave pública.

Descarga de una clave pública

Antes de empezar: Creación de una cuenta de DEP.

1. En la barra de menús, haga clic en **Configuración > Integración externa > Programa de inscripción de dispositivos de Apple**.
2. Haga clic en +.
3. En el paso **2 de 4: Descargar una clave pública**, haga clic en **Descargar clave pública**.

4. Haga clic en **Guardar**.

Después de terminar: Generación de un identificador del servidor.

Generación de un identificador del servidor

Antes de empezar: Descarga de una clave pública.

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

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

Registro del identificador del servidor con BlackBerry UEM

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

Antes de empezar: Generación de un identificador del servidor.

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

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

Adición de la configuración de la primera inscripción

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

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

1. Escriba un nombre para la configuración.
2. Complete una de las tareas siguientes:
   - Si desea que BlackBerry UEM asigne automáticamente la configuración de inscripción a los dispositivos al registrarlos en el Programa de inscripción de dispositivos de Apple, seleccione la casilla para marcar "Asignar automáticamente todos los nuevos dispositivos a esta configuración".

- Si desea utilizar la consola de BlackBerry UEM para asignar manualmente la configuración de inscripción a dispositivos específicos, no seleccione la casilla para marcar "Asignar automáticamente todos los nuevos dispositivos a esta configuración".

3. Opcionalmente, escriba el nombre de un departamento y un número de teléfono de soporte para que se muestren en los dispositivos durante la instalación.
4. En la sección **Configuración del dispositivo**, seleccione entre las siguientes casillas para marcar:
   - Permitir emparejamiento: si esta opción está seleccionada, los usuarios pueden emparejar el dispositivo con un ordenador
   - Obligatorio: si esta opción está seleccionada, los usuarios pueden activar los dispositivos mediante su nombre de usuario y contraseña del directorio de la empresa
   - Permitir la eliminación del perfil de MDM: si esta opción está seleccionada, los usuarios pueden desactivar los dispositivos.
   - Espere hasta que se haya realizado la configuración del dispositivo: si esta opción está seleccionada, los usuarios no pueden cancelar la configuración del dispositivo hasta que la activación con BlackBerry UEM haya finalizado.
5. En la sección **Omitir durante la configuración**, seleccione los elementos que no desea incluir en la instalación del dispositivo:
   - Código de acceso: si esta opción está seleccionada, a los usuarios no se les solicita que creen un código de acceso del dispositivo
   - Servicios de ubicación: si esta opción está seleccionada, los servicios de ubicación se desactivan en el dispositivo
   - Restaurar: si esta opción está seleccionada, los usuarios no pueden restaurar datos de un archivo de copia de seguridad
   - Mover desde Android: si esta opción está seleccionada, no puede restaurar los datos desde un dispositivo Android
   - ID de Apple: si esta opción está seleccionada, los usuarios no pueden iniciar sesión en ID de Apple y iCloud
   - Términos y condiciones: si esta opción está seleccionada, los usuarios no ven los términos y condiciones de iOS.
   - Siri: si esta opción está seleccionada, Siri se desactiva en los dispositivos
   - Diagnóstico: si esta opción está seleccionada, la información de diagnóstico no se envía automáticamente desde el dispositivo durante la instalación
   - Biométrico: si esta opción está seleccionada, los usuarios no pueden configurar Touch ID
   - Pago: si esta opción está seleccionada, los usuarios no pueden configurar Apple Pay
   - Zoom: si esta opción está seleccionada, los usuarios no pueden configurar zoom
   - Configuración del botón de inicio: cuando está seleccionado, los usuarios no pueden ajustar el clic del botón de inicio
   - Tiempo en pantalla: si se selecciona, la opción para configurar el tiempo en pantalla se omitirá durante la inscripción en DEP
   - Actualización de software: si se selecciona, los usuarios no verán la pantalla de actualización de software obligatoria en el dispositivo
   - iMessage y Face Time: si se selecciona, los usuarios no verán las pantallas de iMessage y Face Time en el dispositivo
   - Tono para mostrar: si se selecciona, los usuarios no verán la pantalla de Tono para mostrar en el dispositivo
   - Privacidad: si se selecciona, los usuarios no verán la pantalla Privacidad en el dispositivo
   - Integración: si se selecciona, los usuarios no verán la pantalla informativa de integración en el dispositivo
   - Migración de Watch: si se selecciona, los usuarios no verán la pantalla de migración de Watch en el dispositivo

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

6. Haga clic en **Guardar**.

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

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

Actualización del identificador del servidor

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

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

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

Eliminar conexión de DEP

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

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

1. En la barra de menús, haga clic en **Configuración > Integración externa > Programa de inscripción de dispositivos de Apple**.
2. Haga clic en **Eliminar conexión de DEP**.
3. Haga clic en **Eliminar**.
4. Haga clic en **Aceptar**.

Configuración de BlackBerry UEM para que admita dispositivos Android Enterprise

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

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

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

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

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

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

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

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

Para obtener información acerca de la configuración de BlackBerry UEM y la compatibilidad con Chrome OS, consulte Ampliación de la administración de dispositivos Chrome OS a BlackBerry UEM.

Configurar BlackBerry UEM para que sea compatible con dispositivos Android Enterprise

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

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

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 **Bring Android to Work**, inicie sesión con una cuenta de Google. Puede utilizar cualquier cuenta de Google o de Gmail. La cuenta que utilice se convertirá en la cuenta de administrador para el servicio **Utilizar Android en el trabajo**. **d.** Haga clic en **Comenzar**. **e.** Escriba el nombre de su empresa Haga clic en **Confirmar**. **f.** Haga clic en **Completar registro**. Volverá a la consola de gestión de BlackBerry UEM.

Tarea	Pasos
Utilizar un dominio de Google	a. Seleccione **Conectar BlackBerry UEM a su dominio de Google existente**. Tenga en cuenta que no puede compartir dominios de Google entre varios dominios de BlackBerry 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**. Para obtener instrucciones detalladas, visite support.blackberry.com/community y lea el artículo 37748.

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

Eliminación de la conexión con el dominio de Google

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

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

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

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

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

4. Haga clic en **Eliminar**.

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

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

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

Edición o prueba de la conexión de dominio de Google

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

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

Ampliación de la gestión de dispositivos Chrome OS a BlackBerry UEM

La compatibilidad de Chrome OS con BlackBerry UEM requiere un dominio gestionado de Google. 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. La integración de Chrome OS con BlackBerry UEM amplía la gestión de algunas de las funciones de gestión de Chrome OS a UEM.

En la consola de administración de Google, los usuarios y los dispositivos se organizan en unidades de organización, que son una representación jerárquica de grupos de usuarios, dispositivos y configuraciones. BlackBerry UEM sincroniza estas unidades de organización de la consola de administración de Google en grupos de unidades de organización de UEM. Para obtener más información sobre las unidades organizativas, consulte la información de Google.

Una vez Google BlackBerry UEM finalizada la sincronización entre y, UEM se registra con el Google dominio para recibir notificaciones de cambios en unidades de organización, usuarios o dispositivos. A continuación, si, por ejemplo, se inscribe un dispositivo, el nombre de un usuario cambia o se mueve una unidad de organización, se envía una notificación inmediatamente a UEM y se actualiza la base de datos en consecuencia.

Si UEM el entorno de su empresa ya está configurado para Android Enterprise, puede agregar otra conexión que pueda utilizar para administrar los Chrome OS dispositivos.

Para obtener más información, visite support.blackberry.com y lea el artículo 98789.

Nota: Su dominio gestionado por Google debe incluir "Chrome Enterprise Upgrade".

Configuración de la gestión de dispositivos Chrome OS si ya ha configurado BlackBerry UEM para utilizar Android Enterprise

Si ya utiliza Android Enterprise, solo necesita realizar estos pasos para preparar la administración de dispositivos Chrome OS en BlackBerry UEM:

- Asegúrese de que el dominio Google de su empresa tenga Chrome OS habilitado para la empresa
- Asegúrese de que la API de política Chrome está activada en el dominio Google de su empresa. Para obtener más información, consulte Creación de una cuenta de servicio que BlackBerry UEM utilice para autenticarse con su dominio de Google Cloud o Google Workspace by Google
- Asegúrese de que se han añadido todos los ámbitos. Para obtener más información, consulte Activar las API adicionales para permitir que BlackBerry UEM sincronice los datos de Chrome OS
- Active en Chrome OS la consola de administración BlackBerry UEM. Consulte Sincronización de BlackBerry UEM con la consola de administración de Google

Cree una cuenta de servicio que BlackBerry UEM utilice para autenticarse con su dominio Google Cloud o Google Workspace by 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 gestionar el proyecto.

2. Haga clic en **Crear proyecto**.
3. Escriba un nombre para el proyecto.
4. Haga clic en **Crear**.
5. Una vez creado el proyecto, haga clic en el mismo y, en el panel izquierdo, expanda **IAM y administración** y haga clic en **Cuentas de servicio**.
6. Haga clic en **Crear cuenta de servicio**.
7. Escriba un nombre para la cuenta de servicio y haga clic en **Crear y continuar**.
8. En la lista **Función**, seleccione **Básica > Editor.**
9. Haga clic en **Continuar**.
10. Haga clic en **Hecho**.
11. Seleccione su cuenta de servicio.
12. Haga clic en la pestaña **Claves**.
13. Haga clic en **Agregar clave > Crear nueva clave > P12 > Crear**.
14. Copie la contraseña de la clave privada, la utilizará más adelante.
15. Es posible que se le solicite que descargue el certificado o se descargará automáticamente. Localícelo y guárdelo en una carpeta conocida.
16. Haga clic en **Cerrar**.
17. Haga clic en ≡ > **Cuentas de servicio**.
18. En la columna **Acciones**, haga clic en > **Administrar detalles**.
19. Copie el **ID único de cliente** y la **dirección de correo** para la cuenta del servicio. Pegue esta información en el mismo archivo de texto en el que pegó la contraseña de la clave privada para usarla más adelante en el proceso.
20. Haga clic en ≡ > **API y servicios > API y servicios habilitados**.
21. Haga clic en **Habilitar API y servicios**.
22. Busque y seleccione **API Administrar SDK**.
23. Haga clic en **Activar**.
24. Busque y seleccione **EMM API de Google Play**.
25. Haga clic en **Activar**.
26. Busque y seleccione **API de política de Chrome**.
27. Haga clic en **Activar**.

Activar API adicionales para permitir a BlackBerry UEM 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.

1. Inicie sesión en la consola de administración de Google con la cuenta de administrador de su dominio de Google.
2. Vaya a **Inicio > Dispositivos > Dispositivos móviles y puntos finales > Configuración > Integración con servicios de terceros**.
3. Haga clic en **EMM de Android** y asegúrese de haber seleccionado **Habilitar gestión de dispositivos móviles Android por parte de terceros**.
4. Haga clic en **Agregar proveedores de EMM > Generar token**.

5. Copie el token. Péguelo en el mismo archivo de texto en el que pegó la contraseña de clave privada.
6. Cierre las ventanas del token y haga clic en **Guardar**.
7. Haga clic en **Guardar de todos modos**.
8. Haga clic en **Seguridad > Control de acceso y datos > Controles de API**.
9. En **Delegación de dominios**, haga clic en **ADMINISTRAR DELEGACIÓN DE DOMINIOS**.
10. Haga clic en **Agregar nuevo** (junto a Clientes de API).
11. En el campo **ID de cliente**, pegue el ID de cliente único de la cuenta de servicio de Google que registró anteriormente e introduzca las siguientes direcciones en el campo Ámbitos de OAuth, en una lista separada 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.device.chromeos
    - https://www.googleapis.com/auth/admin.directory.device.mobile
    - https://www.googleapis.com/auth/admin.directory.orgunit
    - https://www.googleapis.com/auth/admin.directory.user
    - https://www.googleapis.com/auth/chrome.management.policy
    - https://www.googleapis.com/auth/admin.reports.audit.readonly
12. Haga clic en **Autorizar**.
    Nota: Al autorizar esta API para la cuenta de servicio permite a UEM acceder al directorio de usuario para Google Cloud o Google Workspace mediante el dominio de Google.

Integrar BlackBerry UEM con un dominio de Google Cloud o de Google Workspace by Google de forma que pueda usar dispositivos con Chrome OS

1. Inicie sesión en la consola de administración de UEM con una cuenta de administrador de seguridad.
2. En la barra de menú, haga clic en **Configuración > Integración externa > Android Enterprise**.
3. Seleccione **Conectar BlackBerry UEM a su dominio de Google existente**. Tenga en cuenta que no puede compartir dominios de Google entre varios dominios de BlackBerry UEM. Esta opción es compatible con Android Enterprise y Chrome OS Enterprise.
4. En la sección 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 Google Developers Console.
7. Al lado del campo **Archivo del certificado P12**, haga clic en **Examinar**.
8. Desplácese hasta el archivo de certificado recibido de Google Developers Console y haga clic en **Abrir**.
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 que copió de Google Developers Console.
10. En el campo **Dirección de correo electrónico para el administrador de dominios de Google**, escriba la dirección de correo electrónico de la cuenta de administrador que utilice para gestionar el dominio de Google Cloud o de Google Workspace by Google.
11. En el campo **Token**, pegue el token que ha generado en el dominio de Google.
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 Cloud o un dominio de Google Workspace by Google.

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. Haga clic en **Siguiente**.

Sincronizar BlackBerry UEM con la consola de administración de Google

Tras sincronizar BlackBerry UEM con su dominio de Google, puede llevar a cabo algunas acciones de administración en los dispositivos con Chrome OS de su empresa, como activar, desactivar y anular las tareas de administración.

1. Inicie sesión en la consola de administración de UEM con una cuenta de administrador de seguridad.
2. En la barra de menú, haga clic en **Configuración > Integración externa > Android Enterprise**.
3. En la sección de administración de Chrome OS, haga clic en **Activar**. Este botón realiza una sincronización inicial de datos en 10 minutos y también programa sincronizaciones a intervalos regulares.
   Nota: Una vez finalizada la sincronización, puede utilizar los botones **Sincronizar unidades de organización, Sincronizar usuarios** y **Sincronizar dispositivos** para llevar a cabo sincronizaciones fuera de horario.

Simplificación de activaciones de Windows 10

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

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

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

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

Integración de UEM con la combinación Azure Active Directory

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

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

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

Integración de UEM con la combinación de Azure Active Directory

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

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

13. Haga clic en **Guardar**.

Configuración de Windows Autopilot en Microsoft Azure

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

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

Creación de un perfil de implementación de Windows Autopilot en Azure

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

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

Importación de dispositivos Windows Autopilot a Azure

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

16. Reinicie Apache Tomcat.

Configuración de BlackBerry UEM Cloud para admitir las aplicaciones de BlackBerry Dynamics

Siga las instrucciones de esta sección para configurar BlackBerry UEM Cloud para que admita las aplicaciones de BlackBerry Dynamics.

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

Gestión de clústeres de BlackBerry Proxy

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

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

Tarea	Pasos
Cree un nuevo clúster de BlackBerry Proxy.	**a.** Haga clic en +. **b.** Escriba un nombre para el clúster. **c.** Haga clic en **Guardar**.
Cambie el nombre del clúster de BlackBerry Proxy.	**a.** Haga clic en un nombre de clúster. **b.** Cambie el nombre de clúster. Cada clúster debe tener un nombre único. **c.** Haga clic en **Guardar**.
Mueva una instancia de BlackBerry Proxy a un clúster de BlackBerry Proxy diferente.	**a.** En la columna **Servidores**, haga clic en el nombre de una instancia de BlackBerry Proxy. **b.** En la lista desplegable **Clúster de** BlackBerry Proxy, seleccione el clúster en el que desea agregar la instancia. **c.** Haga clic en **Guardar**.
Elimine un clúster de BlackBerry Proxy vacío.	**a.** Haga clic en × de ese clúster. **b.** Haga clic en **Eliminar**.

Tarea	Pasos
Establecimiento de la configuración de proxy de la aplicación para un clúster	**a.** Haga clic en **Configuración > BlackBerry Dynamics > Clústeres**. **b.** Haga clic en el nombre del clúster. **c.** Haga clic en **Anular configuración global**. Consulte Configuración de los ajustes de proxy de la aplicación BlackBerry Dynamics para BlackBerry Cloud Connector para obtener más información.
Descarga de actualizaciones del archivo PAC para todos los clústeres	• Haga clic en **Actualizar caché de PAC**
Especificación de un certificado raíz de confianza para descargar archivos PAC del servidor	**a.** Verifique que el certificado tiene el formato X.509 (*.cer y *.der) y guárdelo en una ubicación de red a la que pueda acceder desde la consola de gestión. **b.** En la barra de menús, haga clic en **Configuración > Integración externa > Certificados de confianza**. **c.** Haga clic en +, ubicado junto a **Elementos de confianza del servidor PAC**. **d.** Haga clic en **Examinar**. **e.** Seleccione el archivo de certificado que desea utilizar. **f.** Haga clic en **Abrir**. **g.** Escriba una descripción para el certificado. **h.** Haga clic en **Agregar**.

Configuración de Direct Connect utilizando reenvío de puertos

Antes de empezar:

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

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

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

6. Haga clic en **Guardar**.

Conexión de BlackBerry Proxy a BlackBerry Dynamics NOC

Si tiene previsto utilizar BlackBerry Proxy para permitir que las aplicaciones de BlackBerry Dynamics puedan conectarse a los recursos de la empresa, el firewall de la empresa debe permitir las conexiones TCP a los rangos de IP que se indican a continuación, para que BlackBerry Proxy pueda conectarse al NOC de BlackBerry Dynamics:

- 206.124.114.1 a 206.124.114.254 (206.124.114.0/24) en el puerto 443
- 206.124.121.1 a 206.124.121.254 (206.124.121.0/24) en el puerto 443
- 206.124.122.1 a 206.124.122.254 (206.124.122.0/24) en el puerto 443

De forma alternativa, puede configurar el firewall de su empresa para permitir conexiones a los siguientes nombres de host:

- gdentgw.good.com en el puerto 443
- gdrelay.good.com en el puerto 443
- gdweb.good.com en el puerto 443
- gdmdc.good.com en el puerto 443

Conexión de BlackBerry UEM a un conector PKI de BlackBerry Dynamics

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

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

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

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

1. En la barra de menús, haga clic en **Configuración > Integración externa > Autoridad de certificación**.
2. Haga clic en **Agregar una conexión de PKI de BlackBerry Dynamics**.
3. En el campo **Nombre de la conexión**, escriba un nombre para la conexión.
4. En el campo **URL**, escriba la URL del conector de PKI.
5. Seleccione una de las siguientes opciones:
   - **Autenticar con nombre de usuario y contraseña**: elija esta opción si BlackBerry UEM se autentica con el conector de PKI de BlackBerry Dynamics mediante la autenticación basada en contraseña.

- **Autenticar con certificado de cliente**: elija esta opción si BlackBerry UEM se autentica con el conector de PKI de BlackBerry Dynamics mediante la autenticación basada en certificado.

6. Si ha seleccionado **Autenticar con nombre de usuario y contraseña**, en los campos **Nombre de usuario** y **Contraseña**, escriba el nombre de usuario y la contraseña del conector de PKI de BlackBerry Dynamics.
7. Si ha seleccionado **Autenticar con certificado de cliente**, haga clic en **Examinar** para seleccionar y cargar un certificado que sea de confianza para el conector de PKI de BlackBerry Dynamics. En el campo **Contraseña del certificado de cliente**, escriba la contraseña del certificado.
8. En la sección **Certificado de confianza para el conector PKI** puede especificar el certificado que utiliza BlackBerry UEM para establecer conexiones de confianza con el conector PKI, seleccione una de las siguientes opciones:
   - **Certificado de CA de BlackBerry Control TrustStore**
   - **Certificado de CA**: si selecciona esta opción, deberá hacer clic en Examinar para seleccionar el certificado de CA de la empresa.
   - **Certificado de servidor de conector PKI**: si selecciona esta opción, deberá hacer clic en Examinar para seleccionar el certificado de servidor de conector PKI de la empresa.
9. Para probar la conexión, haga clic en **Probar conexión**.
10. Haga clic en **Guardar**.

Después de terminar:

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

Anulación de la configuración de proxy HTTP general para un BlackBerry Connectivity Node

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

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

Consideraciones del archivo PAC

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

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

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

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

- BLOCK (consideradas como DIRECT)
- SOCKS (se producirá un error de conexión)
- SOCKS4 (se producirá un error de conexión)
- SOCKS5 (se producirá un error de conexión)
- HTTP (se producirá un error de conexión)
- La directiva "NATIVE" personalizada definida por BlackBerry Access (se producirá un error de conexión)

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

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

Nota:

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

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

Configuración de los ajustes de proxy de la aplicación BlackBerry Dynamics para BlackBerry Cloud Connector

Puede configurar los ajustes de proxy de BlackBerry Cloud Connector de las aplicaciones de BlackBerry Dynamics manualmente o utilizando un archivo PAC.

1. En BlackBerry Cloud Connector, haga clic en **Configuración general > BlackBerry Router y proxy**.
2. Seleccione **Configuración general**.
3. Seleccione una de las siguientes opciones:
   - **Activar proxy HTTP manual**
   - **Activar PAC**

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

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

b) Si los servidores proxy especificados en el archivo PAC requieren autenticación, seleccione **Admitir autenticación proxy** y especifique el **Nombre de usuario**, la **Contraseña** y, si es necesario, el **Dominio** que debe utilizar la aplicación para la autenticación.

   Las credenciales de autenticación de usuario final no son compatibles para la autenticación proxy.

6. Haga clic en **Guardar**.

Configurar las notificaciones de correo electrónico para BlackBerry Work

BEMS Cloud acepta solicitudes de registro de inserción de los dispositivos, como por ejemplo iOS y Android, y luego establece una comunicación con el servidor Microsoft Exchange Server o Microsoft Office 365 local para comprobar si se han producido cambios en el buzón de correo del usuario. Cuando se especifica la información del servidor Microsoft Exchange Server o Microsoft Office 365 local, se especifica la configuración para crear el inquilino de BEMS Cloud para su empresa.

Cuando se crea el inquilino, los servicios que se indican a continuación se activan automáticamente:

- BlackBerry Directory Lookup: este servicio permite que los usuarios puedan buscar a otros usuarios por su nombre, su apellido y la foto o el avatar que tienen asociados en el directorio de la empresa.
- BlackBerry Follow-Me: esta función admite BlackBerry Dynamics Launcher en BlackBerry Work.

Un entorno de autenticación híbrido moderno (por ejemplo, en entornos locales de Microsoft Exchange Server y Microsoft Office 365), permite que las instalaciones Microsoft Exchange Server utilicen una autenticación y autorización de usuario más seguras mediante el consumo de identificadores de acceso OAuth obtenidos de la nube. Para obtener más información acerca de cómo configurar un Microsoft Exchange Server local para utilizar una autenticación moderna híbrida, visite https://docs.microsoft.com/en-us/microsoft-365/enterprise/configure-exchange-server-for-hybrid-modern-authentication?view=o365-worldwide.

Antes de empezar: Compruebe que dispone de la siguiente información y que ha completado las tareas correspondientes.

- Verifique que la cuenta de servicio tiene permisos de suplantación de aplicaciones aplicados.
- Si dispone de un entorno híbrido de Microsoft Office 365 y un entorno local de Microsoft Exchange Server, y habilita el modo de autenticación moderno, asegúrese de que el Microsoft Exchange Server local está configurado para utilizar el modo de autenticación híbrido moderno. Para obtener más información, visite https://docs.microsoft.com/en-us/microsoft-365/enterprise/configure-exchange-server-for-hybrid-modern-authentication?view=o365-worldwide. Si Microsoft Exchange Server no se configura correctamente, los usuarios no recibirán notificaciones por correo electrónico.
- En un entorno de Microsoft Office 365, si quiere activar la autenticación moderna, asegúrese de haber realizado lo siguiente:
  - Si activa la autenticación moderna mediante la autenticación de credenciales, obtenga el ID de aplicación de cliente.
  - Si activa la autenticación moderna mediante la autenticación de certificados de cliente, realice una de las siguientes acciones:
    - Obtenga el ID de aplicación de cliente con autenticación basada en certificados
    - Cree y asocie un certificado .pfx autofirmado al ID de aplicación de Azure para BEMS
  - Si ha configurado el acceso condicional de Azure AD para su empresa, asegúrese de que BlackBerry Connectivity Node esté instalado y configurado en su entorno.
  - Configurar las notificaciones de correo electrónico para BlackBerry Work
  - En un entorno local de Microsoft Exchange, asegúrese de que Microsoft Exchange Server se actualiza para que sea compatible con TLS 1.2 o las notificaciones de inserción fallarán. Los paquetes de cifrado más

débiles, como TLSv1 o TLS 1.0, están desactivados de forma predeterminada. La desactivación de los paquetes de cifrado proporciona una seguridad mejorada.

- Si utiliza la autenticación pasiva, compruebe que tiene el ID de aplicación de BEMS mediante la autenticación de credenciales.
- Si utiliza SSL para la búsqueda de SCP, compruebe que ha exportado el certificado SSL de Microsoft Active Directory.

1. En la consola de gestión, haga clic en **Configuración > BlackBerry Dynamics > Notificaciones de correo electrónico**.
2. En la sección **Tipo de autenticación**, seleccione un tipo de autenticación basado en su entorno y complete las tareas asociadas para permitir que BEMS se comunique con Microsoft Exchange Server o Microsoft Office 365:

Tipo de autenticación	Descripción	Tarea
Credencial	Esta opción utiliza un nombre de usuario y una contraseña de BEMS definidos para autenticarse en Microsoft Exchange Server o Microsoft Office 365 mediante la autenticación básica.	**a.** En el campo **Nombre de usuario de la cuenta de servicio**, escriba el nombre de usuario de la cuenta de servicio de BEMS. • En Microsoft Office 365, introduzca el nombre principal de usuario (UPN) de la cuenta de servicio. • En el Microsoft Exchange Server local, utilice el formato <*dominio*>\<*nombre de usuario*>. **b.** En el campo **Contraseña de la cuenta de servicio**, introduzca la contraseña de la cuenta de servicio.
Certificado de cliente	Esta opción utiliza un certificado de cliente para permitir que la cuenta de servicio de BEMS autentique Microsoft Exchange Server o Microsoft Office 365.	**a.** Junto al campo **Archivo de certificado (.pfx)**, haga clic en **Examinar**. Desplácese y seleccione el archivo de certificado de cliente. **b.** En el campo **Contraseña**, escriba la contraseña del certificado de cliente.

Tipo de autenticación	Descripción	Tarea
Autenticación pasiva	Esta opción utiliza un proveedor de identidad (IDP) para autenticar al usuario y proporcionar identificadores de OAuth a BEMS para autenticarse con Microsoft Office 365. En un entorno híbrido, la autenticación se realiza en un Microsoft Exchange Server local.*	**a.** En el campo **Autoridad de autenticación**, introduzca la URL del servidor de autenticación a la que BEMS accede y de la que recupera el identificador de OAuth para la autenticación con Microsoft Office 365 (por ejemplo, https://login.microsoftonline.com/common). **b.** En el campo **ID de aplicación de cliente**, introduzca el ID de aplicación de Azure para la autenticación de credenciales. Para obtener instrucciones, consulte el ID de aplicación de BEMS mediante la autenticación de credenciales. **c.** En el campo **Nombre del servidor**, escriba el FQDN del servidor de Microsoft Office 365. De forma predeterminada, el nombre del servidor es https://outlook.office365.com. **d.** En el campo **URI de redirección** se muestra la URL a la que el IDP redirige al administrador cuando se autoriza el ID de aplicación de cliente y se proporcionan los identificadores de autenticación. Este campo se rellena previamente con la información de la partición y no se puede modificar. **e.** Haga clic en **Iniciar sesión**. **f.** Escriba las credenciales de la cuenta de servicio. **g.** Haga clic en **Aceptar** para confirmar que se han obtenido los identificadores de autenticación. **h.** Importante: BEMS Cloud no actualiza automáticamente los identificadores de OAuth. Repita los pasos de la "e" a "g" para actualizar los identificadores de OAuth. La caducidad de los identificadores depende de la directiva de inquilino (de forma predeterminada, la caducidad de los identificadores es de 90 días). Cuando los identificadores de OAuth caducan, las notificaciones por correo electrónico de los dispositivos de los usuarios se detienen. La caducidad del identificador de OAuth se muestra después de iniciar sesión en el IDP.

* El Microsoft Exchange Server local debe estar configurado para utilizar la autenticación híbrida moderna. Para obtener más información, visite https://docs.microsoft.com/en-us/microsoft-365/enterprise/configure-exchange-server-for-hybrid-modern-authentication?view=o365-worldwide.

3. Si se conecta a un entorno de Microsoft Office 365, realice lo siguiente para activar la autenticación moderna:
   a) Marque la casilla de verificación **Permitir autenticación moderna**.
   b) En el campo **Autoridad de autenticación**, introduzca la URL del servidor de autenticación a la que BEMS accede para recuperar el identificador de OAuth para la autenticación en Microsoft Office 365 (por ejemplo, https://login.microsoftonline.com/<*nombre de inquilino*> o https://login.microsoftonline.com/<*ID de inquilino*>).
   c) En el campo **ID de aplicación de cliente**, introduzca uno de los siguientes ID de aplicación de Azure, en función del tipo de autenticación que haya seleccionado. Realice una de las siguientes acciones para obtener un ID de aplicación de Azure:
      - Obtener el ID de aplicación de Azure para BEMS con autenticación pasiva o de credenciales
      - Obtención de un ID de aplicación de Azure para BEMS con autenticación basada en certificados

d) En el campo **Nombre del servidor**, introduzca el FQDN del servidor de Microsoft Office 365 (por ejemplo, https://outlook.office365.com).
e) De forma opcional, también puede seleccionar la casilla de verificación **Utilizar las credenciales si la autenticación moderna falla** para permitir que BEMS se comunique con Microsoft Office 365 en el caso de que BEMS no pueda acceder a la fuente de autenticación moderna. Al marcar esta casilla de verificación, deberá introducir las credenciales de la cuenta de servicio de BEMS.

Nota: Cuando se configura la autenticación moderna, todos los nodos utilizan la configuración especificada.

4. En el campo **Nombre de usuario de la cuenta de servicio**, introduzca el nombre de usuario asignado para iniciar sesión en el servidor Microsoft Exchange Server o Microsoft Office 365. El nombre de usuario debe utilizar uno de los formatos siguientes:
   - Si su entorno utiliza un Microsoft Exchange Server local, utilice <*Dominio*>\<*Nombre de usuario*> o el UPN.
   - Si su entorno utiliza Microsoft Office 365, utilice <*nombre de usuario*>@<*dominio*>.com.
5. En el campo **Contraseña de la cuenta de servicio**, introduzca la contraseña correspondiente al nombre de usuario de la cuenta de servicio que se introdujo previamente.
6. Opcionalmente, en el campo **Omitir URL de detección automática**, introduzca la URL de detección automática para que BEMS pueda obtener la información de usuario del servidor Microsoft Exchange Server o Microsoft Office 365 cuando detecte usuarios para BlackBerry Push Notifications.

   Nota: Si no se introduce ninguna, BEMS utiliza la función de detección automática para localizar el servidor Microsoft Exchange Server o Microsoft Office 365 y obtener la información de usuario.
7. Marque la casilla de verificación **Permitir la redirección HTTP y el registro de servidores DNS** para permitir la redirección HTTP y la búsqueda de servidores DNS para recuperar la URL de detección automática durante el proceso de detección de usuarios para BlackBerry Push Notifications. De forma predeterminada, esta función está activada.
8. Seleccione **Utilizar ruta de BlackBerry Connectivity Node** para permitir que BEMS Cloud se conecte a Microsoft Exchange Server o Microsoft Office 365 mediante la red corporativa en lugar de utilizando una conexión directa desde la infraestructura de BlackBerry BEMS. Esta configuración requiere que BlackBerry Connectivity Node esté instalado y configurado en su entorno. Si su entorno utiliza el acceso condicional Azure AD, asegúrese de que esta opción esté seleccionada.
9. Si su entorno utiliza una URL interna para acceder y comunicarse con el Microsoft Exchange Server local, seleccione la casilla de verificación **Utilizar URL de Servicios Web de Exchange interna**. Esta configuración requiere que la opción "Utilizar ruta de BlackBerry Connectivity Node" esté activada. Esta opción no está disponible si la autenticación moderna está activada.
10. Opcionalmente, active la casilla de verificación **Activar búsqueda de SCP** para consultar Microsoft Active Directory mediante LDAP y localizar la URL del extremo de detección automática. Esta configuración solo es válida si está seleccionada la autenticación "Credencial" y si BlackBerry Connectivity Node está instalado y configurado en su entorno. Esta opción no está disponible si se ha seleccionado "Omitir URL de detección automática".
11. Active la casilla de verificación **Activar SSL para SCP**. Esto permite que BEMS pueda comunicarse con Microsoft Active Directory mediante SSL. Esta configuración requiere que esté seleccionada la opción "Activar búsqueda de SCP". Si activa esta función, debe agregar el certificado SSL de Microsoft Active Directory a la base de datos de BEMS Cloud. Para obtener información sobre cómo agregar el certificado, consulte Crear una conexión de confianza entre BEMS Cloud y Microsoft Exchange Server.
12. Si ha activado **Activar búsqueda de SCP** o **Activar búsqueda de SCP** y **Activar SSL para SCP**, especifique los **Controladores de dominio para SCP** para configurar LDAP a través de SCP. Si tiene varios controladores de dominio, separe los controladores de dominio con comas (por ejemplo, controladordedominio1.ejemplo.com, controladordedominio2.ejemplo.com, etc.).
13. Opcionalmente, en el campo **Dirección de correo electrónico del usuario:**, se puede introducir una dirección de correo electrónico para probar la conexión con el servidor Microsoft Exchange Server o Microsoft Office 365.

Haga clic en **Probar conexión**. Si la prueba falla, resuelva los problemas identificados e inténtelo de nuevo. Puede eliminar la dirección de correo electrónico después de completar la prueba.

14. Haga clic en **Guardar**.

Después de terminar:

- Pruebe la conexión con el servidor Microsoft Exchange Server o Microsoft Office 365 locales y la función de detección automática. Actualice o vuelva a abrir la pantalla de notificaciones de correo electrónico. Haga clic en **Probar conexión**.
  Nota: Asegúrese de que la prueba de conexión se realiza correctamente antes de aprovisionar los dispositivos para evitar problemas de detección automática. Si los dispositivos se han activado antes de configurar el servicio de notificación de correo electrónico, pida a los usuarios de BlackBerry Work que cierren la sesión y vuelvan a iniciarla. Si la prueba devuelve un mensaje de error, complete las tareas para resolver el problema y vuelva a probar la conexión.
- Asigne la autorización de BlackBerry Cloud Enterprise Services (com.blackberry.gdservice-entitlement.cloud) a los usuarios para que reciban notificaciones de correo electrónico de BlackBerry Work. Para obtener instrucciones, consulte el siguiente contenido de administración:
  - Asignación de una aplicación a un grupo de usuarios
  - Asignación de un grupo de aplicaciones a un grupo de usuarios
  - Asignación de una aplicación a una cuenta de usuario
  - Asignación de un grupo de aplicaciones a una cuenta de usuario
- Opcionalmente, cree una conexión de confianza entre BEMS Cloud y Microsoft Exchange Server. Para obtener instrucciones, consulte Crear una conexión de confianza entre BEMS Cloud y Microsoft Exchange Server.
- Configure BlackBerry Work. Para obtener instrucciones, consulte el contenido de administración de BlackBerry Work, Notes y Task.
- Opcionalmente, configure el servicio de BEMS-Docs. Para obtener instrucciones, consulte Activación del servicio BEMS-Docs.

Concesión de permisos de suplantación de aplicaciones a la cuenta de servicio

Para que el servicio BlackBerry Push Notifications monitorice los buzones de correo para buscar actualizaciones, la cuenta de servicio de BlackBerry Push Notifications debe tener permisos de suplantación.

Ejecute el siguiente comando de Microsoft Exchange Management Shell para aplicar los permisos de suplantación de aplicaciones a la cuenta de servicio :

- Concesión de permisos de suplantación de aplicaciones utilizando el Centro de administración de Exchange
- Concesión de permisos de suplantación de aplicaciones mediante Microsoft Exchange Management Shell

Concesión de permisos de suplantación de aplicaciones utilizando el Centro de administración de Exchange

1. En función del entorno, inicie sesión en una de las siguientes consolas:

Consola	Pasos
Consola del Centro de administración de Exchange de Microsoft Office 365	**a.** Inicie sesión en https://portal.office.com. **b.** Haga clic en el icono Iniciador de aplicaciones, ubicado en la esquina superior izquierda. **c.** Haga clic en **Administrar**. **d.** En el menú de la consola **Centro de administración de Microsoft 365**, haga clic en **Mostrar todo**. **e.** En la sección **Centros de administración**, haga clic en **Todos los centros de administración**. **f.** Haga clic en **Exchange**.
Consola web del Centro de administración de Microsoft Exchange local	**a.** En un navegador, abra `https://<url_del_servidor_de_acceso_de_clientes_local>/ecp` e inicie sesión con una cuenta válida.

2. Haga clic en **Permisos**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el grupo de funciones.
5. En la sección **Funciones**, haga clic en +. Haga clic en **ApplicationImpersonation > Agregar > Aceptar**.
6. En la sección **Miembros**, haga clic en +. Haga clic en la cuenta que quiere añadir y, a continuación, haga clic en **Añadir > Aceptar**.

Concesión de permisos de suplantación de aplicaciones mediante Microsoft Exchange Management Shell

1. Abra Microsoft Exchange Management Shell.
2. Escriba `New-ManagementRoleAssignment -Name:<ImpersonationAssignmentName> -Role:ApplicationImpersonation -User:<ServiceAccount>`. Por ejemplo, `New-ManagementRoleAssignment -Name:BlackBerryAppImpersonation -Role:ApplicationImpersonation -User:BEMSAdmin`.

Después de terminar:

Para obtener más información sobre cómo restringir los derechos de suplantación de aplicaciones para usuarios específicos, unidades organizativas o grupos de seguridad, visite la Biblioteca de MSDN y consulte Cómo: Configurar suplantación.

Obtener el ID de aplicación de Azure para BEMS con autenticación pasiva o de credenciales

1. Inicie sesión en portal.azure.com.
2. En la columna izquierda, haga clic en **Azure Active Directory**.
3. Haga clic en **App registrations**.
4. Haga clic en **Nuevo registro**.
5. En el campo **Nombre**, escriba un nombre para la aplicación.
6. Seleccione un tipo de cuenta compatible.
7. En la sección **URI de redirección**, en la lista desplegable, lleve a cabo una de las tareas siguientes. El URI de redirección es la URL a la que se redirige el usuario después de autenticarse correctamente en el proveedor de identidad (IDP). **Importante**: Asegúrese de que la URL de redirección coincide con la URL del panel de control o de lo contrario, puede que la autenticación no funcione como se espera.

- Para la autenticación de credenciales, seleccione **Web** e introduzca `https://localhost:8443`.
- Para la autenticación pasiva, seleccione **Cliente público/nativo (móvil y escritorio)** e introduzca la URL que utiliza para acceder al panel de control de BEMS.
  - Si accede al panel de control de BEMS desde el ordenador que aloja la instancia de BEMS, introduzca `https://localhost:8443`.
  - Si accede al panel de control de BEMS de forma remota, introduzca `https://<FQDN del ordenador que aloja la instancia de BEMS>:8443`.

8. Haga clic en **Registrar**. Se muestra entonces la nueva aplicación registrada.
9. En la sección **Gestionar**, haga clic en **Permisos de API**.
10. En la sección **Permisos configurados**, si se muestra Microsoft Graph, haga clic en **Microsoft Graph**. Si no se muestra, agregue **Microsoft Graph**.
11. Configure los siguientes permisos:
    - Para Microsoft Exchange Web Services: Acceder a buzones como usuario con sesión iniciada a través de Servicios Web Exchange (**EWS > EWS.AccessAsUser.All**)
    - Para Microsoft Graph: para iniciar sesión y leer el perfil de usuario (**Usuario > User.Read**).
12. haga clic en una de las siguientes opciones:
    - Si el permiso de API de Microsoft Graph existía en la lista de permisos de API, haga clic en **Actualizar permisos**.
    - Si necesita agregar el permiso de API de Microsoft Graph, haga clic en **Crear**.
13. Haga clic en **Conceder consentimiento de administrador**. Haga clic en **Sí**.

    Importante: Este paso requiere privilegios de administrador del inquilino.
14. Para que la detección automática funciones según lo previsto, configure los permisos de autenticación.
    a) En la sección **Gestionar**, haga clic en **Autenticación**.
    b) En la sección **Permitir flujos de cliente públicos**, seleccione **Sí** para **Activar los siguientes flujos de escritorio y móvil**.
    c) Haga clic en **Guardar**.
15. Haga clic en **Información general**. Copie el **ID de aplicación (cliente)**. El ID de aplicación (cliente) se muestra en la página principal **Información general** de la aplicación específica. Se utiliza como el **ID de aplicación de cliente** cuando se activa la autenticación moderna y se configura BEMS para comunicarse con Microsoft Office 365.

Obtención de un ID de aplicación de Azure para BEMS con autenticación basada en certificados

1. Inicie sesión en portal.azure.com.
2. En la columna izquierda, haga clic en **Azure Active Directory**.
3. Haga clic en **App registrations**.
4. Haga clic en **Nuevo registro**.
5. En el campo **Nombre**, escriba un nombre para la aplicación.
6. Seleccione un tipo de cuenta compatible.
7. Opcionalmente, en la sección **Redirigir URI**, en la lista desplegable, seleccione **Público/cliente (móvil y escritorio)** e introduzca http://<*nombre de la aplicación indicada en el paso 5*>.

   Esta aplicación es un daemon, no una aplicación web, por lo que no dispone de una URL de registro.
8. Haga clic en **Registrar**. Se muestra entonces la nueva aplicación registrada.
9. En la sección **Gestionar**, haga clic en **Permisos de API**.
10. Haga clic en **Agregar un permiso**.
11. En la sección **Seleccionar una API**, haga clic en **API que utiliza mi organización**.

12. Haga clic en **Office 365 Exchange Online**.
13. Establezca los siguientes permisos para Office 365 Exchange Online:
    - Permisos de aplicación: usar los servicios Web de Exchange con acceso completo a todos los buzones de correo (**full_access_as_app**)
14. Haga clic en **Agregar permisos**.
15. Haga clic en **Microsoft Graph**. Si el permiso de API de Microsoft Graph no aparece en la lista, agréguelo.
16. Configure los siguientes permisos para Microsoft Graph.
    - Permisos delegados: iniciar sesión y leer el perfil de usuario (**Usuario > User.Read**)
17. Haga clic en **Agregar permisos**.
18. Haga clic en **Conceder consentimiento de administrador**.
19. Haga clic en **Sí**.
20. Haga clic en **Descripción general** para ver la aplicación que ha creado en el paso 5. Copie el **ID de la aplicación (cliente)**. El ID de la aplicación (cliente) se muestra en la página principal de **Descripción general** de la aplicación específica. Se utiliza como el **ID de la aplicación de cliente** en el panel de control de BEMS cuando se activa la autenticación moderna y se configura BEMS para comunicarse con Microsoft Office 365.

Después de terminar: Asociación de un certificado con el ID de aplicación de Azure para BEMS

Asociación de un certificado con el ID de aplicación de Azure para BEMS

Puede utilizar un certificado existente desde el servidor de CA o mediante el comando New-SelfSignedCertificate para crear un certificado autofirmado. Para obtener más información, visite docs.microsoft.com y consulte New-SelfSignedCertificate.

Antes de empezar: Compruebe que dispone del nombre de la aplicación que ha asignado en BEMS con la autenticación basada en certificados.

1. Si dispone de un certificado emitido por un servidor de CA, vaya al paso 2. Cree un certificado autofirmado.
   a) En un ordenador con Microsoft Windows, abra Windows PowerShell.
   b) Introduzca el siguiente comando: `$cert=New-SelfSignedCertificate -Subject "CN=<nombre de la aplicación>" -CertStoreLocation "Cert:\CurrentUser\My" -KeyExportPolicy Exportable -KeySpec Signature`.
      - <*app name*> es el nombre que asignó a la aplicación en el paso 5 de Obtención de un ID de aplicación de Azure para BEMS con autenticación basada en certificados
   c) Pulse **Intro**.
2. Exporte el certificado desde el Administrador de certificados. Se creará el certificado público. Asegúrese de guardar el certificado público como archivo .CER o .PEM.
   a) En el ordenador con Windows, abra el Administrador de certificados para el usuario conectado.
   b) Expanda **Personal**.
   c) Haga clic en **Certificados**.
   d) Haga clic con el botón derecho en <*usuario*>@<*dominio*> y seleccione **Todas las tareas > Exportar**.
   e) En el **Asistente para exportar certificados**, haga clic en **No exportar la clave privada**.
   f) Haga clic en **Siguiente**.
   g) Seleccione **Base-64 encoded X.509 (.CER)**. Haga clic en **Siguiente**.
   h) Ponga un nombre al certificado y guárdelo en el escritorio.
   i) Haga clic en **Siguiente**.
   j) Haga clic en **Finalizar**.
   k) Haga clic en **Aceptar**.

3. Cargue el certificado público para asociar las credenciales de certificado con el ID de aplicación de Azure para BEMS.
   a) En el portal.azure.com, abra el <*nombre de la aplicación*> que asignó a la aplicación en el paso 5 de Obtención de un ID de aplicación de Azure para BEMS con autenticación basada en certificados
   b) Haga clic en **Configuración > Claves**.
   c) Haga clic en **Cargar clave pública**.
   d) Haga clic en y vaya a la ubicación a la que exportó el certificado en el paso 2.
   e) Haga clic en **Abrir**.
   f) Haga clic en **Guardar**.

Después de terminar: Exporte el certificado en formato .pfx mediante el complemento MMC de gestión de certificados de usuario. Asegúrese de incluir la clave privada. Para obtener instrucciones, visite docs.microsoft.com y consulte Exportar un certificado con la clave privada.

Crear una conexión de confianza entre BEMS Cloud y Microsoft Exchange Server

De forma predeterminada, BEMS solo tiene en cuenta los certificados de CA públicos. Si activa las notificaciones por correo electrónico para BlackBerry Work y el Microsoft Exchange Server de su empresa no utiliza un certificado SSL emitido por una CA de confianza, la conexión entre BEMS Cloud y Microsoft Exchange Server no será de confianza. Para crear una conexión de confianza a Microsoft Exchange Server, cargue el certificado SSL del servidor (o la raíz o la cadena de certificados intermedia) en la base de datos de BEMS Cloud. Puede cargar un archivo codificado base64 o binario que incluya uno o más certificados SSL. Si carga un único archivo que incluya varios certificados SSL, los certificados se muestran en la consola de administración y se pueden eliminar y sustituir individualmente según sea necesario. BEMS Cloud admite las siguientes extensiones de archivo: .der, .cer, .pem y .crt.

Antes de empezar:

- Configure las notificaciones de correo electrónico para BlackBerry Work Para obtener instrucciones, consulte Configurar las notificaciones de correo electrónico para BlackBerry Work.
- Exporte el certificado SSL de Microsoft Exchange Server en formato codificado base64 o binario y guárdelo en una ubicación de red a la que pueda acceder desde la consola de administración. Para obtener más información sobre certificados digitales y cifrado en Microsoft Exchange Server, visite https://docs.microsoft.com/en-us/exchange/architecture/client-access/certificates?view=exchserver-2016

1. En la barra de menú, haga clic en **Configuración > BlackBerry Dynamics**.
2. Haga clic en **Notificaciones de correo electrónico**.
3. Haga clic en la pestaña **Certificados**.
4. Haga clic en .
5. Haga clic en **Agregar**.
6. Haga clic en **Examinar** y busque la ubicación del certificado que desea cargar.
7. Haga clic en **Agregar**.
8. Si carga certificados SSL individuales, repita los pasos del 5 al 7 con cada archivo adicional.

Sustituir o eliminar los certificados SSL de la conexión de confianza

Al sustituir los certificados SSL (por ejemplo, cuando los certificados caduquen), sustituya todos los certificados SSL existentes en la base de datos de BEMS. Puede optar por cargar certificados SSL individuales según sea necesario o incluir varios certificados SSL en un único archivo. Se admiten los siguientes tipos de archivo: .der, .cer, .pem y .crt.

Antes de empezar:

- Exporte los certificados SSL nuevos de Microsoft Exchange Server en formato codificado base64 o binario y guárdelos en una ubicación de red a la que pueda acceder desde la consola de administración. Para obtener más información sobre certificados digitales y cifrado en Microsoft Exchange Server, visite https://docs.microsoft.com/en-us/exchange/architecture/client-access/certificates?view=exchserver-2016

1. En la barra de menú, haga clic en **Configuración > BlackBerry Dynamics**.
2. Haga clic en **Notificaciones de correo electrónico**.
3. Haga clic en la pestaña **Certificados**.
4. Haga clic en .
5. Haga clic en **Eliminar**, ubicado bajo el certificado que desea eliminar.
6. Haga clic en **Eliminar** para confirmar la eliminación.
7. Agregue el certificado nuevo. Para obtener instrucciones, consulte Crear una conexión de confianza entre BEMS Cloud y Microsoft Exchange Server.

Configure el mensaje de advertencia de caducidad de la contraseña

En caso de un usuario Active Directory y de grupos de usuarios que utilicen el método PSO (objeto de configuración de contraseña) para establecer la antigüedad máxima de la contraseña, puede configurar BEMS Cloud para permitir que las aplicaciones de los usuarios de BlackBerry Work muestren un mensaje de advertencia cuando su contraseña de Active Directory esté a punto de caducar.

Nota: En la consola de administración de BlackBerry UEM, las notificaciones de correo electrónico de BlackBerry Work deben configurarse mediante el tipo de autenticación de credencial para mostrar la pestaña Vencimiento de contraseña.

Para obtener información sobre cómo mostrar un mensaje de advertencia para los usuarios que utilizan el método GPO (objeto de política global) para establecer la antigüedad máxima de la contraseña, consulte el contenido de administración de BlackBerry Work.

Antes de empezar:

- Asegúrese de disponer de la siguiente información:
  - Credenciales de inicio de sesión para la cuenta de servicio que se utiliza para autenticar el controlador de dominio.
  - Nombre del servidor LDAP y número de puerto. El nombre del servidor LDAP debe ser uno de los controladores de dominio.
- Compruebe que la cuenta de servicio tenga permisos de lectura READ para el "contenedor de configuración de contraseña". Para obtener instrucciones, consulte Adición de permiso de lectura a la cuenta utilizada para autenticarse en el servidor LDAP.
- Compruebe que BlackBerry Connectivity Node está instalado y configurado en su entorno. Para obtener más información, consulte Pasos para instalar y activar BlackBerry Connectivity Node.
- Compruebe que los administradores utilizan el método PSO para establecer la antigüedad máxima de la contraseña para los usuarios.
- Compruebe que los usuarios en su entorno estén ejecutando BlackBerry Work 3.8 o posterior.

1. En la consola de gestión, haga clic en **Configuración > BlackBerry Dynamics > Notificaciones de correo electrónico**.
2. Haga clic en la pestaña **Caducidad de la contraseña**.
3. Haga clic en .
4. Seleccione la casilla de verificación **Activar caducidad de la contraseña** para permitir que BEMS consulte a Active Directory los detalles de caducidad de la contraseña para los usuarios.

5. En el campo **Nombre de servidor LDAP**, introduzca el nombre del servidor LDAP (por ejemplo, ldap.<*DNS_domain_name*>).
6. En el campo **Puerto LDAP**, escriba el número de puerto del ordenador de LDAP. El puerto predeterminado es el 389.
7. Introduzca la cuenta de inicio de sesión de LDAP y la contraseña. Puede introducir la cuenta de inicio de sesión en el formato `dominio\nombredeusuario` o Nombre principal de usuario (UPN) `nombredeusuario@dominio`.
8. En el campo **DN de base (controlador de dominio)**, introduzca el DN de base para la búsqueda de LDAP. Si esta entrada no está establecida, BEMS intenta encontrar el DN base en el atributo namingContexts.
9. Opcionalmente, seleccione la casilla **Activar LDAP de SSL** para tunelizar los datos a través de una conexión cifrada SSL. Si activa LDAP de SSL, introduzca el número de puerto en el equipo LDAP que utilizó en el paso 6. El puerto predeterminado es el 636. Este paso requiere que importe el certificado de LDAP en el almacén de claves de BEMS. Para obtener instrucciones, consulte Crear una conexión de confianza entre BEMS Cloud y Microsoft Exchange Server.
10. Haga clic en **Test** para comprobar la conexión con el servidor de LDAP.
11. Haga clic en **Guardar**.

Adición de permiso de lectura a la cuenta utilizada para autenticarse en el servidor LDAP

Puede utilizar la herramienta Editor ADSI de Windows para agregar permisos de lectura a la cuenta que se utiliza para autenticarse en el servidor LDAP. Debe ser miembro del grupo Administradores de dominio o tener permisos equivalentes para completar esta tarea.

1. Inicie la utilidad Editor ADSI.
2. Haga clic con el botón derecho del ratón en el icono **Editor ADSI** y haga clic en **Conectar a**.
3. En la pantalla **Configuración de conexión**, en la sección **Punto de conexión**, seleccione **Seleccionar un contexto de nomenclatura conocido** y, en la lista desplegable, seleccione **Contexto de nomenclatura predeterminado**.
4. Haga clic en **Aceptar**.
5. Haga clic en su dominio.
6. Desplácese hasta **CN =Sistema** y expanda.
7. Haga clic derecho en **CN=Contenedor de configuración de contraseñas** y haga clic en **Propiedades**.
8. En la pestaña **Seguridad**, haga clic en **Agregar** para agregar la cuenta, o el grupo de usuarios del que es miembro la cuenta, que se utiliza para autenticarse en el servidor LDAP.
9. En **Nombres de grupos o usuarios**, con la cuenta o grupo de usuarios agregados seleccionados, active la casilla de verificación **Lectura** en la columna **Permitir**.
10. Haga clic en **Aplicar**.
11. Haga clic en **Aceptar**.

Configuración de BlackBerry Dynamics Launcher

BlackBerry Dynamics Launcher es un componente de interfaz de usuario al que se puede acceder mediante las aplicaciones de BlackBerry Dynamics (por ejemplo, BlackBerry Work) con el botón de BlackBerry Dynamics Launcher. BlackBerry Dynamics Launcher crea una ubicación de marcador de posición para la configuración de la aplicación. BlackBerry Dynamics Launcher es un módulo de la biblioteca con numerosas funciones, que actualmente incluye lo siguiente:

- El nombre, la foto, la presencia y el estado del usuario

- Una lista de las aplicaciones con tecnología de BlackBerry Dynamics y los módulos instalados en el dispositivo.
- Opciones de creación rápida para redactar un correo electrónico, crear una nota, programar un evento de calendario o agregar un contacto, independientemente de la aplicación que esté abierta actualmente.

En la consola de gestión de BlackBerry UEM, las notificaciones de correo electrónico de BlackBerry Work deben configurarse para mostrar BlackBerry Dynamics Launcher y se debe definir un icono personalizado para BlackBerry Dynamics Launcher en los dispositivos del usuario.

Configuración de un icono personalizado para BlackBerry Dynamics Launcher

Puede especificar un icono personalizado predeterminado para BlackBerry Dynamics Launcher en los dispositivos de los usuarios. Cuando especifica un icono personalizado, el icono sustituye al icono de BlackBerry Dynamics de todos los usuarios gestionados por la instancia de BEMS.

Cuando especifique un icono personalizado, asegúrese de que el archivo cumple los siguientes requisitos:

- Menos de 500 KB. Los iconos de más de 500 KB no se agregan a la lista de iconos personalizados.
- Nombre con el siguiente formato: <*nombre archivo*>_<*tipo_dispositivo*>_<*resolución*>.png. Por ejemplo, Icono_iOS_2x.png.

  Donde *resolución* es la resolución que admite el dispositivo. Por ejemplo:

  - Dispositivos Android: ldpi, mdpi, hdpi, xhdpi, xxhdpi y xxxhdpi
  - Dispositivos iOS: 1x, 2x, 3x, etc.
- Guardado en formato .png

Especificación de un icono personalizado para BlackBerry Dynamics Launcher

BEMS Cloud permite especificar un icono personalizado para los usuarios de su entorno. Al agregar iconos personalizados, BEMS Cloud verifica la validez de las imágenes cargadas. Para obtener más información acerca de los requisitos de los iconos personalizados, consulte Configuración de un icono personalizado para BlackBerry Dynamics Launcher.

Antes de empezar:

- Compruebe que las notificaciones de correo electrónico para BlackBerry Work están configuradas.
- Compruebe que tiene acceso a un icono personalizado compatible para BlackBerry Dynamics Launcher. Para obtener más información acerca de los requisitos del archivo, consulte Configuración de un icono personalizado para BlackBerry Dynamics Launcher.

1. En la consola de gestión de BlackBerry UEM, en la barra de menús, haga clic en **Configuración > BlackBerry Dynamics > Marca de Launcher**.
2. Seleccione la casilla de verificación **Mostrar icono personalizado en Launcher**.
3. Haga clic en la pestaña del dispositivo para el que desea especificar el icono de Launcher. Android está seleccionado de forma predeterminada.
4. Haga clic en +.
5. Desplácese a la ubicación del archivo del icono. Haga clic en el archivo y, a continuación, en **Abrir**.
6. Haga clic en **Submit**.
7. Haga clic en **Guardar**.
8. Repita los del 4 al 6 para cada resolución de archivo de icono de los dispositivos con Android personalizada.
9. Siga los del 3 al 6 para cada resolución de archivo de icono de los dispositivos con iOS personalizada.

Eliminación de un icono personalizado de BlackBerry Dynamics Launcher

Puede eliminar un icono personalizado que haya especificado para BlackBerry Dynamics Launcher. Si elimina todos los archivos de iconos personalizados, se utilizará el icono de Launcher predeterminado para la aplicación Launcher en los dispositivos de cliente.

1. En la consola de administración de BlackBerry UEM, en la barra de menú, haga clic en **Configuración > BlackBerry Dynamics > Marca de Launcher**.
2. Haga clic en la pestaña del dispositivo del que desea eliminar el icono personalizado de Launcher.
3. Haga clic en ✕, que se encuentra junto al icono personalizado que desea eliminar.
4. Haga clic en **Guardar**.

Configuración de BEMS-Docs

Puede utilizar la consola de BlackBerry UEM para configurar y mantener repositorios de documentos y archivos, y políticas de acceso para usuarios de aplicaciones móviles del servicio. Cuando se activa, los usuarios pueden acceder a los documentos, sincronizarlos y compartirlos utilizando los siguientes servicios de almacenamiento: Microsoft SharePoint Online, Microsoft SharePoint, Microsoft OneDrive for Business y Box. No se admiten proveedores de almacenamiento de repositorios basados en CMIS y recurso compartido de archivo.

Nota: Si su entorno requiere que los usuarios accedan a repositorios basados en CMIS o recurso compartido de archivo, configure BEMS-Docs en una instancia local de BEMS. No se admite la activación de BEMS-Docs en BlackBerry UEM Cloud y en una instancia local de BEMS en un entorno de BlackBerry UEM Cloud. Para obtener más información, consulte Configuración de un BEMS local en un entorno de BlackBerry UEM Cloud.

Repositorios: el servicio BEMS-Docs ofrece a los usuarios acceso a los datos de trabajo almacenados desde sus dispositivos móviles. Existe un repositorio de Docs (también llamado "recurso compartido") en un servidor de trabajo. El repositorio contiene archivos compartidos por usuarios autorizados. Para obtener más información acerca de la configuración y el mantenimiento de los recursos compartidos en BlackBerry UEM y el acceso de usuarios asociado, consulte Gestión de repositorios. Antes de configurar los repositorios, active y configure el servicio BEMS-Docs y configure BlackBerry Work en BlackBerry UEM para permitir que los usuarios accedan a los repositorios que agregue y defina desde su dispositivo

Servicios de almacenamiento: el servicio BEMS-Docs es compatible con varios servicios de almacenamiento.

Pasos para configurar BEMS-Docs

Cuando configura BEMS-Docs, realice las acciones siguientes:

Paso	Acción
1	Activación del servicio BEMS-Docs.
2	Configuración de BEMS-Docs.
3	Creación de una conexión de confianza entre BEMS-Docs y Microsoft SharePoint.
4	Gestión de repositorios.

Paso	Acción
5	Asigne el derecho "Feature - Docs Service Entitlement (com.good.feature.share)" a los usuarios para permite que BlackBerry Work Docs se conecte al servicio BEMS-Docs. Para obtener instrucciones, consulte el siguiente contenido de administración: • Asignación de una aplicación a un grupo de usuarios • Asignación de un grupo de aplicaciones a un grupo de usuarios • Asignación de una aplicación a una cuenta de usuario • Asignación de un grupo de aplicaciones a una cuenta de usuario

Activación del servicio BEMS-Docs

Para permitir que los usuarios accedan a los repositorios de documentos y archivos en su entorno, debe activar el servicio BEMS-Docs. Al activar este servicio, se crea un inquilino de BEMS y se agrega la autorización de BlackBerry Cloud Docs Service (com.blackberry.gdservice-entitlement.docs.cloud) al perfil de conectividad de BlackBerry Dynamics. Si su entorno emplea tanto el servicio BEMS-Docs como las notificaciones de correo electrónico para BlackBerry Work, configure primero las notificaciones de correo electrónico. Para obtener instrucciones, consulte Configurar las notificaciones de correo electrónico para BlackBerry Work.

Para activar el servicio BEMS-Docs, la autorización de BlackBerry Cloud Docs Service (com.blackberry.gdservice-entitlement.docs.cloud) debe estar presente en Organización > Autorizaciones en https://account.blackberry.com. No es necesario asignar esta autorización de aplicación a los usuarios en BlackBerry UEM Cloud.

1. En la consola de gestión, haga clic en **Configuración > BlackBerry Dynamics > Docs**.
2. Haga clic en **Activar**.

Configuración de BEMS-Docs

Antes de empezar:

- Compruebe que el servicio BEMS-Docs está activado.
- Si su entorno está configurado para Microsoft SharePoint Online o Azure-IP, asegúrese de que la aplicación BlackBerry Work está registrada en Azure para que pueda acceder a la aplicación BEMS-Docs Azure. Para obtener instrucciones, consulte Obtener un ID de la aplicación Azure para BlackBerry Work en el contenido de administración de BlackBerry Work, Notes y Tasks.
- Si su entorno está configurado para Azure-IP, tenga a mano la siguiente información:
  - Nombre del inquilino de Azure
  - ID de la aplicación Azure del servicio BEMS
  - Clave de la aplicación Azure del servicio BEMS
- Si BEMS-Docs está configurado para comunicarse con una instancia local de Microsoft SharePoint, asegúrese de que los repositorios de Microsoft SharePoint utilizan puertos seguros HTTPS. No se admite el uso de puertos no seguros HTTPS.

1. En la consola de gestión, haga clic en **Configuración > BlackBerry Dynamics > Docs**.
2. Haga clic en la pestaña **Configuración**.
3. Complete una o las dos tareas siguientes:

Entorno	Pasos
Su entorno está configurado para usar Microsoft SharePoint Online o Azure-IP y Microsoft SharePoint Online	**a.** Opcionalmente, seleccione la casilla de verificación **Activar protección de información de Azure** para permitir que BEMS-Docs se autentique en Azure-IP. **b.** Introduzca el nombre del inquilino Azure. **c.** Introduzca del ID de la aplicación Azure del servicio BEMS que obtuvo al registrar el servicio de componente BEMS-Docs. Para obtener instrucciones, consulte Obtener un ID de la aplicación Azure para el servicio de componente BEMS-Docs. **d.** Introduzca la clave de la aplicación Azure del servicio BEMS que obtuvo al registrar la aplicación Docs en Azure. Para obtener instrucciones, consulte Obtener un ID de la aplicación Azure para el servicio de componente BEMS-Docs.
Su entorno está configurado para usar una instancia local de Microsoft SharePoint	**a.** Seleccione la casilla de verificación **Habilitar ruta de BlackBerry Connectivity Node** para permitir que BEMS se conecte a BlackBerry Infrastructure en lugar de utilizar un puerto de entrada. Esta configuración requiere que BlackBerry Connectivity Node esté instalado y configurado en su entorno. **b.** Para permitir que BEMS-Docs se comunique con una instancia local del servidor Microsoft SharePoint, extraiga el certificado del servidor Microsoft SharePoint y envíelo al soporte técnico de BlackBerry. Si los sitios locales de Microsoft SharePoint utilizan certificados que no son públicamente de confianza (por ejemplo, certificados con firma automática o de una CA de empresa), envíe los certificados al soporte técnico de BlackBerry.

4. Haga clic en **Guardar**.

Obtención de un ID de aplicación de Azure para el servicio de componentes de BEMS-Docs

Cuando su entorno está configurado para Microsoft SharePoint Online, Microsoft OneDrive for Business o Microsoft AzureIP, debe registrar los servicios de componente BEMS en Azure.

Si su entorno utiliza tanto Microsoft SharePoint Online y Microsoft Azure-IP o Microsoft OneDrive for Business como Microsoft Azure-IP, debe registrar el servicio Microsoft SharePoint Online o Microsoft OneDrive for Business. Microsoft Azure–IP utilizará la misma información que el servicio registrado.

Antes de empezar: Para conceder permisos, debe usar una cuenta con permisos de administrador del inquilino.

1. Inicie sesión en portal.azure.com.
2. En la columna izquierda, haga clic en **Azure Active Directory**.
3. Haga clic en **App registrations**.
4. Haga clic en **Nuevo registro**.
5. En el campo **Nombre**, escriba un nombre para la aplicación. Por ejemplo, AzureAppIDforBEMS.
6. Seleccione un tipo de cuenta compatible.
7. En la lista desplegable **URI de redireccionamiento**, seleccione **Web** e introduzca `https://localhost:8443`.
8. Haga clic en **Registrar**.
9. Registre el **ID de la aplicación (cliente)**. Se utilizará como valor de **ID de la aplicación BEMS Service Azure** en la consola de gestión de BlackBerry UEM.Se utilizará como valor de **ID de la aplicación BEMS Service Azure** para el servicio Docs > Configuración en el panel de BEMS.

10. En la sección **Gestionar**, haga clic en **Permisos de API**.
11. Haga clic en **Agregar un permiso**.
12. Complete una o varias de las tareas siguientes:

Servicio	Permisos
Si configura BEMS-Docs para utilizar Microsoft SharePoint Online or Microsoft OneDrive for Business	**a.** Busque y haga clic en **SharePoint**. **b.** Configure los siguientes permisos: • En los permisos de aplicaciones, anule la selección de todos los permisos. **1.** Haga clic en **Permisos de aplicaciones**. **2.** Haga clic en expandir todo. Asegúrese de que todas las opciones estén deseleccionadas. • En los permisos delegados, seleccione la casilla de verificación **Leer y escribir en elementos y listas de elementos de todas las colecciones de sitios**. Ninguno. Desmarque las casillas de verificación de todas las opciones. • **Permisos delegados** Seleccione la casilla de verificación **Leer y escribir en elementos y listas de todas las colecciones de sitios**. (**AllSite > AllSites.Manage**) **c.** Haga clic en **Agregar permisos**.

Servicio	Permisos
Si utiliza Microsoft Azure-IP	**a.** Haga clic en **Microsoft Graph**. Si Microsoft Graph no aparece, agregue Microsoft Graph. **b.** Configure los siguientes permisos: • En los permisos de aplicaciones, seleccione la casilla de verificación **Leer datos de directorio** (**Directory > Directory.Read.All**). • En los permisos delegados, seleccione la casilla de verificación **Leer datos de directorio** (**Directory > Directory.Read.All**). **c.** Haga clic en **Actualizar permisos**. **d.** **Agregar un permiso**. **e.** En la sección **Seleccionar una API**, haga clic en **Servicios de administración de derechos de Azure**. Configure los siguientes permisos: • En los permisos de aplicaciones, seleccione todos los permisos. **1.** Haga clic en **Permisos de aplicaciones**. **2.** Asegúrese de que todas las opciones estén seleccionadas. • En los permisos delegados, active la casilla de verificación **user_impersonation**. **f.** Haga clic en **Agregar permisos**. **g.** Haga clic en **Agregar un permiso**. **h.** En la sección **Seleccionar una API**, haga clic en **API que utiliza mi organización**. **i.** Busque y haga clic en **Servicio de sincronización de protección de la información de Microsoft**. Configure el siguiente permiso: • En los permisos delegados, seleccione la casilla de verificación **Leer todas las políticas unificadas a las que tiene acceso un usuario** (**UnifiedPolicy > UnifiedPolicy.User.Read**). **j.** Haga clic en **Agregar permisos**.

13. Espere unos minutos y, a continuación, haga clic en **Conceder permiso de admin**. Haga clic en **Sí**.

Importante: Este paso requiere privilegios de administrador del inquilino.

14. Para que la detección automática funciones según lo previsto, configure los permisos de autenticación. Realice los pasos siguientes:

a) En la sección **Gestionar**, haga clic en **Autenticación**.
b) En la sección **Permitir flujos de clientes públicos**, seleccione **Sí** para **Habilitar los siguientes flujos de escritorio y móvil**.
c) Haga clic en **Guardar**.

15. Defina el ámbito y la confianza de esta API. En la sección **Gestionar**, haga clic en **Exponer una API**. Realice las siguientes tareas.

Tarea	Pasos
Agregar un ámbito	El ámbito restringe el acceso a los datos y la funcionalidad protegidos por la API. **a.** Haga clic en **Agregar un ámbito**. **b.** Haga clic en **Guardar y continuar**. **c.** Complete los siguientes campos y configuraciones: • Nombre de ámbito: Proporcione un nombre único para el ámbito. • Quién puede dar su consentimiento: Haga clic en **Administradores y usuario**. • Nombre para mostrar del consentimiento del administrador: Introduzca un nombre descriptivo. • Descripción del consentimiento del administrador: Escriba un nombre para el ámbito. • Estado: Haga clic en **Activado**. De forma predeterminada, el estado es Activado. **d.** Haga clic en **Agregar ámbito**.
Agregar una aplicación cliente	La autorización de una aplicación cliente indica que la API confía en la aplicación y no se debe solicitar consentimiento a los usuarios. **a.** Haga clic en **Agregar una aplicación cliente**. **b.** En el campo **Id. de cliente**, introduzca el ID de cliente que ha registrado en el paso 9 anterior. **c.** Seleccione la casilla de verificación **Ámbitos autorizados** para especificar el tipo de token que devuelve el servicio. **d.** Haga clic en **Agregar aplicación**.

16. En la sección **Gestionar**, haga clic en **Certificados y secretos** y agregue un secreto de cliente. Realice los pasos siguientes:

a) Haga clic en **Nuevo secreto de cliente**.
b) En el campo **Descripción**, introduzca una descripción de la clave con un máximo de 16 caracteres incluidos espacios.
c) Especifique una fecha de caducidad (por ejemplo, En 1 año, En 2 años o Nunca expira).
d) Haga clic en **Agregar**.
e) Copie el **Valor** de la clave.

Importante: El valor solo está disponible cuando lo crea. No puede acceder a él después de salir de la página. Se utilizará como valor de **Clave de la aplicación BEMS Service Azure** en la consola de BlackBerry UEM.

Permitir la autenticación en BEMS-Docs con una dirección de correo electrónico alternativa

Puede configurar BEMS Cloud para permitir que los usuarios se autentiquen en Microsoft SharePoint Online y Microsoft OneDrive for Business con una dirección de correo electrónico diferente a la que se utilizó para instalar y activar BlackBerry Work. Para activar esta función, póngase en contacto con el servicio de asistencia técnica de BlackBerry.

Creación de una conexión de confianza entre BEMS-Docs y Microsoft SharePoint

De forma predeterminada, BEMS Cloud solo tiene en cuenta los certificados de CA públicos. Si habilita el servicio de BEMS-Docs y la instancia de Microsoft SharePoint local de su empresa no utiliza un certificado SSL emitido por una CA de confianza para sitios HTTPS, la conexión entre el servicio de BEMS-Docs y Microsoft SharePoint local no será de confianza y los usuarios no podrán acceder a los archivos ni a los documentos de la aplicación de Docs de BlackBerry Work. Para crear una conexión de confianza a Microsoft SharePoint, cargue el certificado SSL del servidor si está autofirmado o la raíz o la cadena de certificados intermedia en la base de datos de BEMS Cloud. Puede cargar un archivo codificado base64 o binario que incluya uno o más certificados SSL. Si carga un único archivo que incluya varios certificados SSL, los certificados se muestran en la consola de administración y se pueden eliminar y sustituir individualmente según sea necesario. BEMS Cloud admite las siguientes extensiones de archivo: .der, .cer, .pem y .crt.

Antes de empezar:

- Compruebe que ha activado el servicio de BEMS-Docs.
- Exporte el certificado SSL del servidor de Microsoft SharePoint en formato codificado base64 o binario y guárdelo en una ubicación de red a la que pueda acceder desde la consola de administración.

1. En el menú, haga clic en **Configuración > BlackBerry Dynamics > Docs**.
2. Haga clic en la pestaña **Certificado**.
3. Haga clic en **Agregar** y vaya a la ubicación del archivo de certificado que desea cargar.
4. Haga clic en **Agregar**.
5. Si cargar falla, resuelva el problema identificado e inténtelo de nuevo.
6. Si carga certificados SSL individuales, repita los pasos del 3 al 4 con cada archivo adicional.

Sustitución o eliminación del certificado de conexión de confianza de BEMS-Docs

Al sustituir los certificados SSL (por ejemplo, cuando los certificados caduquen), sustituya los certificados SSL existentes en la base de datos de BEMS Cloud. Puede optar por cargar certificados SSL individuales según sea necesario o incluir varios certificados SSL en un único archivo. Se admiten los siguientes tipos de archivo: .der, .cer, .pem y .crt.

Antes de empezar: Exporte los certificados SSL nuevos de Microsoft SharePoint local en formato codificado base64 o binario y guárdelos en una ubicación de red a la que pueda acceder desde la consola de administración.

1. En el menú, haga clic en **Configuración > BlackBerry Dynamics > Docs**.
2. Haga clic en la pestaña **Certificado**.
3. Haga clic en **Eliminar**, ubicado bajo el certificado que desea eliminar. Haga clic en **Eliminar**.
4. Agregue los nuevos archivos de certificado según sea necesario. Para obtener instrucciones, consulte Creación de una conexión de confianza entre BEMS-Docs y Microsoft SharePoint.

Gestión de repositorios

BEMS Cloud tiene los siguientes proveedores de almacenamiento de repositorios:

Repositorio de almacenamiento	Descripción
SharePoint SharePoint Online	Un servidor web seguro que contiene archivos compartidos a los que se accede a través de Internet. Si su entorno está configurado para Microsoft OneDrive for Business, se utiliza el repositorio de almacenamiento de SharePoint Online.
Box	Una cuenta de almacenamiento en nube seguro proporcionada por box.com que contiene archivos compartidos a los que se puede acceder a través de Internet.

Un repositorio se categoriza más en el servicio BEMS-Docs según quien lo ha agregado y definido.

Repositorio de almacenamiento	Descripción
Definido por el administrador	Sitios de proveedores de almacenamiento agregados y mantenidos por los administradores de BlackBerry UEM para los que se ha concedido acceso a usuarios individuales y grupos de usuarios.
Definido por el usuario	Sitios agregados por usuarios finales individuales desde sus dispositivos móviles para los que usted, como administrador de BlackBerry UEM, puede rescindir y restituir el acceso basado en móvil de acuerdo con sus políticas de uso aceptable de TI de la empresa.

Configuración de repositorios

La página Configuración de repositorios contiene las siguientes tres pestañas que puede configurar:

Pestañas	Descripción
Definido por el administrador	Le permite crear y gestionar repositorios, agregar y eliminar usuarios y grupos de usuarios, y asignar a usuarios y grupos de usuarios permisos de acceso y uso de los archivos.
Definido por el usuario	Le permite agregar y eliminar usuarios y grupos de usuarios, activar y desactivar la capacidad para crear repositorios definidos por el usuario de usuarios y grupos de usuarios, y conceder y rescindir permisos para realizar una variedad de acciones relacionadas con archivos en sus repositorios definidos por el usuario.
Usuarios	Le permite buscar un usuario en BlackBerry UEM Cloud para ver los repositorios permitidos por ruta o anulación, y quién definió el recurso compartido (por ejemplo, administrador o usuario).

Recursos compartidos definidos por el administrador

Los recursos compartidos son repositorios de documentos para un proveedor de almacenamiento concreto.

A la hora de definir los repositorios, lleve a cabo las acciones siguientes:

Paso	Acción
1	Definir un repositorio.
2	Defina los permisos de acceso de usuarios y grupos de usuarios.

Concesión de permisos de acceso de usuarios

Los permisos de acceso se definen para un solo repositorio o se heredan de una lista de repositorios existente. Los permisos se pueden conceder de forma selectiva a usuarios y grupos de usuarios de un dominio de Microsoft Active Directory existente. Se debe agregar al menos un usuario o grupo de usuarios a la definición de repositorio para configurar permisos de acceso.

La tabla siguiente enumera los permisos de acceso y la configuración predeterminada que están disponibles.

Permiso	Atributos de permisos	Configuración predeterminada
Lista (Examinar)	Ver y examinar el contenido del repositorio (por ejemplo, subcarpetas y archivos) en la lista que se muestra y ordenar las listas por nombre, fecha, tamaño o tipo	Activado
Eliminar archivos	Eliminar archivos del repositorio	Activado
Leer (Descargar)	Descargar archivos del repositorio en el dispositivo del usuario y abrirlos para lectura	Activado
Escribir (Cargar)	Cargar archivos (nuevos/modificados) desde el dispositivo del usuario al repositorio para su almacenamiento	Activado
Caché (Archivos sin conexión)	Almacenar temporalmente una caché de archivos del repositorio en el dispositivo para acceso sin conexión. Puede designar archivos y carpetas para sincronizarlos con la carpeta sin conexión de la aplicación BlackBerry Work Docs de los usuarios.	Activado
Abrir en	Abrir un archivo en una aplicación del dispositivo compatible con el formato	Activado
Crear carpeta	Agregar nuevas carpetas al repositorio	Activado
Copiar/Pegar	Copiar el contenido del archivo del repositorio y pegarlo en una archivo diferente o una aplicación	Activado
Registrar/ Desproteger	Cuando se desprotege un archivo, el usuario puede editarlo, cerrarlo, volver a abrirlo o trabajar con el archivo sin conexión. Otros usuarios no pueden cambiar el archivo o ver los cambios hasta que se vuelve a registrar	Activado (solo SharePoint)

Permiso	Atributos de permisos	Configuración predeterminada
Generar vínculo compartido	Los usuarios pueden generar un vínculo a un archivo y carpeta y enviar el vínculo a destinatarios Generar vínculo compartido requiere una aplicación BlackBerry Work actualizada.	Activado (solo Box)

Cambiar los permisos de acceso

1. En la consola de gestión, haga clic en **Configuración > BlackBerry Dynamics > Docs**.
2. Haga clic en **Repositorios**.
3. Haga clic en la pestaña **Definido por el administrador**.
4. Haga clic en un repositorio.
5. En **Permisos de acceso**, junto al usuario o grupo de usuarios, active o desactive la casilla de verificación de permisos que desea cambiar.
6. Haga clic en ⊗ junto a cada usuario o grupo de usuarios que desea eliminar.
7. Haga clic en **Guardar**.

Definir un repositorio

Los usuarios y grupos de BlackBerry UEM se deben agregar a una definición de repositorio antes de poder configurar los permisos de acceso. Los usuarios y grupos que se agregan automáticamente reciben los permisos de acceso predeterminados.

Antes de empezar: Para que los usuarios accedan a sus repositorios de Microsoft SharePoint en sus dispositivos, asegúrese de que tienen el nivel de permiso "Leer" y el permiso "Examinar directorios" asignados.

1. En la consola de gestión, haga clic en **Configuración > BlackBerry Dynamics > Docs**.
2. Haga clic en **Repositorios**.
3. Haga clic en la pestaña **Definido por el administrador**.
4. Haga clic en +.
5. En el campo **mostrar**, escriba el nombre del repositorio que se mostrará a los usuarios a los que se ha concedido acceso móvil al repositorio.

   El nombre del repositorio debe ser único y puede contener espacios. Los siguientes caracteres especiales no se pueden usar debido a limitaciones de terceros:

   - Microsoft SharePoint 2010, 2013, 2016 y 2019: ~ " # % & * : < > ? / \ { | }
   - Box: \ /|
6. En la lista desplegable **Almacenamiento**, seleccione un proveedor de almacenamiento.

   Si selecciona **SharePoint** o **SharePoint Online** y el recurso compartido está ejecutando SharePoint 2013 o posterior, seleccione la casilla de verificación **Agregar sitios seguidos por usuarios a este sitio** para que esta opción esté disponible para los usuarios de este recurso compartido. Esta configuración se aplica únicamente a sitios de SharePoint o OneDrive for Business personales (my).

   Si su entorno está configurado para Microsoft OneDrive for Business, seleccione el proveedor de almacenamiento SharePoint Online.
7. En el campo **Ruta**, especifique la ruta al recurso compartido. Lleve a cabo una de las siguientes tareas según el tipo de almacenamiento seleccionado en el paso 6.

Las siguientes variables son compatibles en el campo ruta:

- nombre de usuario
- sAMAccountName
- mail
- dnsDomain
- Si el sitio personal incluye nombres de usuario, introduzca la ruta incluyendo estas variables. Por ejemplo, https://sharepoint.example.com/my/<sAMAccountName>.

Tipo de almacenamiento	Descripción
Box	Introduzca una URL completa con o sin las variables admitidas mencionadas anteriormente.
SharePoint SharePoint Online	Si su proveedor de almacenamiento es Microsoft OneDrive for Business, complete esta tarea. Introduzca una URL completa con o sin las variables admitidas mencionadas anteriormente. Para agregar sitios de SharePoint "my" o personales, especifique la URL del sitio "my". Por ejemplo: • Si su entorno utiliza SharePoint y SharePoint Online, https://<*Microsoft SharePoint server*>/my. • Si su entorno utiliza Microsoft OneDrive for Business, *https://<your O365 domain>-my.sharepoint.com/personal/admin_<domain>_onmicrosoft_com/_layouts/15/onedrive.aspx* Opcionalmente, para agregar automáticamente sitios seguidos, lleve a cabo los siguientes pasos: **a.** Agregue un repositorio al sitio de SharePoint "my" o personal. **b.** Seleccione **Agregar sitios seguidos por los usuarios a este sitio** para el repositorio. **c.** En la pestaña **Definido por el usuario**, active el permiso de repositorios definidos por el usuario. Asegúrese de seleccionar las casillas de verificación **Activar "recursos compartidos definidos por el usuario"** y **Agregar automáticamente sitios seguidos por los usuarios**. Para obtener instrucciones, consulte Activar permisos de repositorios definidos por el usuario.

8. En la sección **Permisos de acceso**, haga clic en +.
9. Seleccione una de las siguientes opciones:
   - **Usuarios**: en el cuadro de diálogo **Agregar un usuario**, escriba una cadena de búsqueda completa o parcial. Haga clic en el usuario que desea agregar.
   - **Grupos**: en la pantalla **Agregar un grupo**, seleccione uno o más grupos. Haga clic en →. Haga clic en **Agregar**.
10. Haga clic en **Agregar**.
11. Haga clic en **Guardar**. Si se produce un error al guardar y se determina el problema, se mostrará el mensaje de error correspondiente (por ejemplo, si tiene un repositorio denominado Marketing y crea otro repositorio con el

mismo nombre, se mostrará el mensaje de error **Ya existe un repositorio con el nombre Marketing**). Resuelva el problema especificado y vuelva a guardar.

Agregar usuarios y grupos de usuarios a repositorios

Los usuarios y grupos de Microsoft Active Directory se deben agregar a una definición de repositorio antes de poder configurar los permisos de acceso. Los usuarios y grupos agregados automáticamente reciben los permisos de acceso predeterminados.

1. En la consola de gestión, haga clic en **Configuración > BlackBerry Dynamics > Docs**.
2. Haga clic en **Repositorios**.
3. Haga clic en la pestaña **Definido por el administrador**.
4. Haga clic en un repositorio.
5. En **Permisos de acceso**, haga clic en +.
6. Seleccione una de las siguientes opciones:
   - **Usuarios**: en el cuadro de diálogo **Agregar un usuario**, escriba una cadena de búsqueda completa o parcial. Haga clic en el usuario que desea agregar.
   - **Grupos**: en la pantalla **Agregar un grupo**, seleccione uno o más grupos. Haga clic en →. Haga clic en **Agregar**.
7. Haga clic en **Agregar**.
8. Haga clic en **Guardar**.

Después de terminar: Conceda permisos de acceso de usuarios y grupos de usuarios.

Editar un repositorio

1. En la consola de gestión, haga clic en **Configuración > BlackBerry Dynamics > Docs**.
2. Haga clic en **Repositorios**.
3. Haga clic en la pestaña **Definido por el administrador**.
4. Haga clic en un repositorio que desea editar.
5. Realice los cambios necesarios.
6. Haga clic en **Guardar**.

Permitir repositorios definidos por el usuario

Para permitir que los usuarios definan sus propios repositorios, lleve a cabo las acciones siguientes:

1. Activar permisos de repositorios definidos por el usuario
2. Cambiar los permisos de acceso de los usuarios

Activar permisos de repositorios definidos por el usuario

Antes de empezar: Para que los usuarios accedan a sus repositorios de Microsoft SharePoint en sus dispositivos, asegúrese de que tienen el nivel de permiso "Leer" y el permiso "Examinar directorios" asignados.

1. En la consola de gestión, haga clic en **Configuración > BlackBerry Dynamics > Docs**.
2. Haga clic en **Repositorios**.
3. Haga clic en la pestaña **Definido por el usuario**.
4. Seleccione la casilla de verificación **Activar "Recursos compartidos definidos por el usuario"** para permitir que los usuarios móviles definan sus propias fuentes de datos.

5. Opcionalmente, seleccione la casilla de verificación **Agregar automáticamente sitios seguidos por los usuarios** para los repositorios de Microsoft SharePoint autorizados con el plug-in MySite necesario activado.

   Para agregar automáticamente sitios seguidos, lleve a cabo los siguientes pasos:

   a. En la pestaña Definido por el administrador, agregue un repositorio para el sitio de SharePoint "my" o personal. Para obtener instrucciones, consulte Definir un repositorio.
   b. Seleccione **Agregar sitios seguidos por los usuarios a este sitio** para el repositorio.
   c. En la pestaña Definido por el usuario, asegúrese de seleccionar las casillas de verificación **Activar recursos compartidos definidos por el usuario** y **Agregar automáticamente sitios seguidos por los usuarios**.
6. En la sección **Almacenamiento**, seleccione uno o varios servicios de almacenamiento.

   Si no selecciona al menos una opción de almacenamiento, la opción definida por el usuario estará desactivada.
7. En la sección **Permisos de acceso**, haga clic en +.
8. Seleccione **Usuarios** o **Grupos**.
9. Seleccione una de las siguientes opciones:

   - **Usuarios**: en el cuadro de diálogo **Agregar un usuario**, escriba una cadena de búsqueda completa o parcial. Haga clic en el usuario que desea agregar.
   - **Grupos**: en la pantalla **Agregar un grupo**, seleccione uno o más grupos. Haga clic en →. Haga clic en **Agregar**.
10. Haga clic en **Agregar**. Los usuarios y grupos agregados automáticamente reciben los permisos de acceso predeterminados.
11. Haga clic en **Guardar**.

Permisos de acceso

Los permisos se pueden conceder de forma selectiva a usuarios y grupos de usuarios de un dominio de Microsoft Active Directory existente. Se aplican los permisos más restrictivos (definidos por el administrador o definidos por el usuario).

La tabla siguiente enumera los permisos que se conceden de forma predeterminada al agregar usuarios y grupos a los repositorios definidos por el usuario.

Permiso	Atributos de permisos	Configuración predeterminada
Lista (Examinar)	Ver y examinar el contenido del repositorio (por ejemplo, subcarpetas y archivos) en la lista que se muestra y ordenar las listas por nombre, fecha, tamaño o tipo	Activado
Eliminar archivos	Eliminar archivos del repositorio	Activado
Leer (Descargar)	Descargar archivos del repositorio en el dispositivo del usuario y abrirlos para lectura	Activado
Escribir (Cargar)	Cargar archivos (nuevos/modificados) desde el dispositivo del usuario al repositorio para su almacenamiento	Activado

Permiso	Atributos de permisos	Configuración predeterminada
Caché (Archivos sin conexión)	Almacenar temporalmente una caché de archivos del repositorio en el dispositivo para acceso sin conexión Puede designar archivos y carpetas para sincronizarlos con la carpeta sin conexión de la aplicación Docs de BlackBerry Work de los usuarios.	Activado
Abrir en	Abrir un archivo en una aplicación del dispositivo compatible con el formato	Activado
Crear carpeta	Agregar nuevas carpetas al repositorio	Activado
Copiar/Pegar	Copiar el contenido del archivo del repositorio y pegarlo en una archivo diferente o una aplicación	Activado
Registrar/Desproteger	Cuando se desprotege un archivo, el usuario puede editarlo, cerrarlo, volver a abrirlo o trabajar con el archivo sin conexión. Otros usuarios no pueden cambiar el archivo o ver los cambios hasta que se vuelve a registrar	Activado (solo SharePoint)
Agregar nuevos repositorios	Permite agregar nuevos repositorios desde el dispositivo móvil del usuario	Desactivado
Generar vínculo compartido	Los usuarios pueden generar un vínculo a un archivo y carpeta y enviar el vínculo a destinatarios Generar vínculo compartido requiere una aplicación BlackBerry Work actualizada.	Activado (solo Box)

Cambiar los permisos de acceso de los usuarios

1. En la consola de gestión, haga clic en **Configuración > BlackBerry Dynamics > Docs**.
2. Haga clic en **Repositorios**.
3. Haga clic en la pestaña **Definido por el usuario**.
4. En **Permisos de acceso**, junto al usuario o grupo de usuarios, active o desactive la casilla de verificación de permisos que desea cambiar.
5. Haga clic en ⊗ junto a cada usuario o grupo de usuarios que desea eliminar.
6. Haga clic en **Guardar**.

Visualización de los derechos de los repositorio del usuario

En algunos casos, puede que necesite buscar un usuario concreto para revisar qué repositorios están configurados para el acceso, así como los permisos específicos otorgados. Por ejemplo, si un usuario es miembro de un grupo de Microsoft Active Directory configurado para acceder a los repositorios y no aparece individualmente en las configuraciones de los repositorios definidas por el administrador o definidas por el usuario y desea considerar la posibilidad de realizar cambios específicos en los permisos de acceso del usuario.

1. En la consola de gestión, haga clic en **Configuración > BlackBerry Dynamics > Docs**.

2. Haga clic en la pestaña **Repositorios**.
3. Haga clic en la pestaña **Usuarios**.
4. En el campo **Buscar**, empiece por escribir el nombre de la cuenta de Microsoft Active Directory del usuario. Si no ve el usuario que desea, amplíe o reduzca la cadena de búsqueda.
5. Haga clic en el nombre del usuario. En la columna **Definido por** se especifica si el repositorio está definido por el administrador o el usuario.
6. Haga clic en el nombre del repositorio para ver los permisos de acceso del usuario. Para modificar los permisos de acceso, consulte Cambiar los permisos de acceso de los usuarios.
7. Opcionalmente, si el repositorio está definido por el administrador, introduzca una ruta de anulación en el campo **Anular ruta para este usuario**.
8. Opcionalmente, si el repositorio está definido por el usuario, introduzca un nombre nuevo del repositorio en el campo **Nombre del repositorio**.

Configuración de un BEMS local en un entorno de BlackBerry UEM Cloud

Puede configurar un BEMS local para comunicarse con BlackBerry Proxy y autenticar identificadores de GDAuth en un entorno de BlackBerry UEM Cloud. Al configurar un entorno con un BEMS local, los usuarios de iOS y Android podrán utilizar los servicios BEMS-Connect, BEMS-Presence y BEMS-Docs , así como las notificaciones de correo electrónico de BEMS Cloud y el servicio BEMS-Docs en BlackBerry Work.

Si su entorno requiere que los usuarios accedan a repositorios basados en CMIS o recurso compartido de archivo, configure BEMS-Docs en un BEMS local. No se admite la activación de BEMS-Docs en BlackBerry UEM Cloud y en un BEMS local en un entorno de BlackBerry UEM Cloud.

Nota: Solo puede configurar BEMS con un entorno local de BlackBerry UEM o de BlackBerry UEM Cloud a la vez.

Pasos para configurar BlackBerry UEM Cloud para que se comunique con un BEMS local

Al configurar BlackBerry UEM Cloud para que se comunique con un BEMS local, debe realizar las acciones siguientes:

Nota: Puede que algunas de las siguientes tareas ya se hayan completado al configurar BlackBerry UEM Cloud.

Paso	Acción
1	Configure BlackBerry UEM Cloud en su entorno.
2	En la consola de BlackBerry UEM Cloud, instale BlackBerry Connectivity Node o actualícelo a la versión más reciente. 1. Compruebe que su empresa cumple los requisitos previos para la instalación de BlackBerry Connectivity Node 2. Descargue los archivos de instalación y activación de BlackBerry Connectivity Node en la consola de gestión. 3. Instale, active y configure BlackBerry Connectivity Node.
3	Si utiliza Connect, instale y configure los siguientes servicios de BEMS local. Para obtener instrucciones sobre cómo instalar BEMS local, consulte el contenido de instalación de BEMS y el contenido de los servicios de BEMS: • BEMS-Connect • BEMS-Presence • BEMS-Docs

Paso	Acción
4	En el panel de BEMS, Configuración del servidor de BlackBerry Dynamics en BEMS. También puede configurar la comunicación SSL entre BlackBerry Connectivity Node y el BEMS local en el puerto 17433. 1. Exportación del certificado de BlackBerry Proxy al equipo local 2. Importación del certificado al almacén de claves de Windows de BEMS 3. Importación del certificado en el almacén de claves de Java en BEMS **Nota:** Si no configura la comunicación SSL, desmarque la casilla de verificación **Enforce SSL Certificate Validation when communicating with BlackBerry Dynamics**.
5	En el panel de BEMS, Configuración de la conectividad de BEMS con BlackBerry Dynamics.

6	En la consola de BlackBerry UEM Cloud, asigne las aplicaciones de BlackBerry Connect y BlackBerry Presence Service a los usuarios.
	• Puede asignar las aplicaciones mediante uno de los siguientes métodos. Para obtener instrucciones, consulte el siguiente contenido de administración de BlackBerry UEM Cloud:
	  • Asignación de una aplicación a un grupo de usuarios
	  • Asignación de un grupo de aplicaciones a un grupo de usuarios
	  • Asignación de una aplicación a una cuenta de usuario
	  • Asignación de un grupo de aplicaciones a una cuenta de usuario

7	En la consola de BlackBerry UEM Cloud, cree un perfil de conectividad de BlackBerry Dynamics y agregue el servidor de aplicaciones que aloja las aplicaciones BlackBerry Connect, BlackBerry Presence Service y Feature - Docs Service Entitlement.

Importación del certificado al almacén de claves de Windows de BEMS

Para que el servicio de Connect confíe en el certificado del servidor de BlackBerry Proxy, debe importar el certificado de BlackBerry Proxy en el almacén de claves de Windows del servicio de Connect. Repita esta tarea en cada instancia de BEMS.

Antes de empezar: Guarde una copia del certificado ca.cer que exportó en una ubicación adecuada en el ordenador que aloja BEMS. Para obtener instrucciones, consulte Exportación del certificado de BlackBerry Proxy al equipo local.

1. Abra la consola de gestión de Microsoft.
2. Haga clic en **Console Root (Raíz de consola)**.
3. Haga clic en **File > Add/Remove Snap-in (Archivo > Agregar/quitar complemento)**.
4. Haga clic en **Certificados**.
5. Seleccione **Cuenta del ordenador > Equipo local > Aceptar**.
6. Expanda **Certificados (equipo local) > Entidades de certificación raíz de confianza**.
7. Haga clic con el botón derecho en **Certificados** y, a continuación, **Todas las tareas > Importar**.

8. Haga clic en **Siguiente**.
9. Navegue hasta donde haya guardado el certificado que ha exportado (por ejemplo, <*unidad de disco*>:\bemscert\ca.cer). Haga clic en **Abrir**.
10. Haga clic en **Siguiente**.
11. Haga clic en **Finalizar**. Haga clic en **Aceptar**.

Después de terminar: Configure el servicio Core de BEMS para comunicarse con BlackBerry Dynamics. Para obtener instrucciones, consulte Configuración de la conectividad de BEMS con BlackBerry Dynamics.

Importación del certificado en el almacén de claves de Java en BEMS

Para que los servicios de Presence y Docs confíen en el certificado del servidor de BlackBerry Proxy, debe importar el certificado de BlackBerry Connectivity Node. Utilice DBmanager para importar el certificado en el almacén de claves de Java de BEMS. De forma predeterminada, DBmanager se encuentra en la carpeta de instalación en `<unidad de disco>:\GoodEnterpriseMobilityServer<versión>\GoodEnterpriseMobilityServer\DBManager`.

Antes de empezar: Guarde una copia del certificado ca.cer que exportó en una ubicación adecuada en el ordenador que aloja BEMS. Para obtener instrucciones, consulte Exportación del certificado de BlackBerry Proxy al equipo local.

1. En el ordenador que aloja el BEMS local, compruebe que la variable del sistema PATH incluye la ruta al directorio de JAVA.
   a) En un símbolo del sistema, introduzca `set | findstr "Path"`.
   b) Pulse **Intro**.

   Para obtener más información sobre cómo definir la variable del sistema Path, consulte "Configuración de Java Runtime Environment" en el contenido de instalación de BEMS en un entorno de BlackBerry UEM.
2. Realice una copia de seguridad del archivo del almacén de claves de Java. El archivo del almacén de claves de Java se encuentra en `%JAVA_HOME%\lib\security\cacerts`, donde JAVA_HOME se confirma en el paso 1.
3. Importe el certificado raíz de BlackBerry Proxy.
   a) Abra un símbolo del sistema y desplácese hasta la carpeta DBManager. Por ejemplo, si los archivos de instalación se guardan en la carpeta de descargas, introduzca `C:\Users\besadmin\Downloads\GoodEnterpriseMobilityServer<versión>\GoodEnterpriseMobilityServer\DBManager`
   b) Importe el certificado. Introduzca `java -jar dbmanager-<versión>-jar-with-dependencies.jar -moduleName pushnotify -dbType sqlserver -dbName <nombre_de_la_base_de_datos_de_SQL_Server> -dbHost <Nombre del ordenador que aloja la base de datos de SQL> -dbPort 1433 -userName gems_sa -password <contraseña_de_la_cuenta_de_servicio_de_BEMS> -action addcertificate -pemFile "C:\<ruta del archivo pem>\<nombre del certificado>.cer" -alias gdcert`
4. Reinicie el servicio de Good Technology Common Services en Windows Service Manager.

Después de terminar: Configure el servicio Core de BEMS para comunicarse con BlackBerry Dynamics. Para obtener instrucciones, consulte Configuración del servidor de BlackBerry Dynamics en BEMS.

Configuración del servidor de BlackBerry Dynamics en BEMS

Su entorno de BEMS debe estar configurado para que confíe en la entidad de certificación raíz de la configuración HTTPS de BlackBerry Proxy, o bien deberá implementar la solución provisional de Karaf. Para obtener

instrucciones, consulte "Importación y configuración de certificados" en el contenido de configuración de BEMS-Core.

1. En **BlackBerry Enterprise Mobility Server Dashboard**, en **BEMS System Settings**, haga clic en **BEMS Configuration**.
2. Haga clic en **BlackBerry Dynamics**.
3. Realice una de las siguientes acciones:

Tarea	Pasos
Si no se ha definido un servidor de BlackBerry Proxy	**a.** Haga clic en **Add BlackBerry Proxy**. **b.** En el campo **Host Name**, escriba el nombre del host del servidor de BlackBerry Proxy. **c.** En la lista desplegable **Protocol**, seleccione el protocolo utilizado para comunicarse con el servidor de BlackBerry Proxy. • Si selecciona HTTPS, el campo **Port** se rellenará automáticamente con el número 17433. Se trata de un puerto seguro. • Si selecciona HTTP, el campo **Port** se rellenará automáticamente con el número 17080. **Nota:** Si configura su entorno para HTTPS, debe Exportación del certificado de BlackBerry Proxy al equipo local y, a continuación, Importación del certificado en el almacén de claves de Java en BEMS. **d.** Haga en **Test** para realizar una prueba de conexión. **e.** Repita los pasos del 1 al 4 para agregar servidores de BlackBerry Proxy adicionales para garantizar la continuidad de la redundancia.
Si se han definido uno o más servidores de BlackBerry Proxy	No es necesario realizar ninguna acción. Se indican los servidores de BlackBerry Proxy definidos previamente.

4. Marque la casilla de verificación **Apply to other nodes in the BEMS cluster** para comunicar la información del servidor de BlackBerry Proxy a todos los nodos de BEMS del clúster.
5. También puede marcar la casilla de verificación **Enforce the SLL Certificate validation when communicating with BlackBerry Dynamics** cuando utilice el protocolo HTTPS para comunicarse con el servidor de BlackBerry Proxy.
6. Haga clic en **Guardar**.

Configuración de la conectividad de BEMS con BlackBerry Dynamics

1. En **BlackBerry Enterprise Mobility Server Dashboard**, en **BlackBerry Services Configuration**, haga clic en **Connect**.
2. Haga clic en **Service Account**.
3. Introduzca el nombre de usuario y la contraseña de la cuenta de servicio.
4. Haga clic en **Guardar**.
5. Haga clic en **BlackBerry Dynamics**.
6. En el campo **Hostname**, escriba el nombre del host del servidor de BlackBerry Proxy.
7. En el campo **Port**, el número de puerto se rellena automáticamente en función del tipo de comunicación que haya seleccionado.

- Si selecciona HTTP, el campo Port se rellenará con el número 17080.
- Si selecciona HTTPS, el campo Port se rellenará previamente con el número 17433. Se trata de un puerto seguro.

Nota: Si configura su entorno para HTTPS, debe Exportación del certificado de BlackBerry Proxy al equipo local y, a continuación, Importación del certificado al almacén de claves de Windows de BEMS.

8. Haga clic en **Test** para comprobar la conexión con el servidor de BlackBerry Proxy.
9. Haga clic en **Guardar**.

Después de terminar: Si ha seleccionado HTTPS, debe configurar la aplicación BlackBerry Connect para que utilice comunicaciones SSL. Para obtener instrucciones, consulte la sección "Configuración de la aplicación BlackBerry Connect" para modificar su entorno en el contenido de administración de BlackBerry Connect.

Adición de un servidor de aplicaciones que aloja las aplicaciones de derecho a un perfil de conectividad de BlackBerry Dynamics

1. En la barra de menú, haga clic en **Políticas y perfiles**.
2. Haga clic en **Networks and Connections > BlackBerry Dynamics connectivity**.
3. Haga clic en + para crear un nuevo perfil de conectividad, o bien en el perfil de conectividad de BlackBerry Dynamics al que quiera agregar un servidor de aplicaciones.
4. Si es necesario, haga clic en ✎.
5. En **Servidores de aplicaciones**, haga clic en **Agregar**.
6. Seleccione la aplicación **Feature - Docs Service Entitlement** para la que desea agregar un servidor de aplicaciones.
7. Haga clic en **Guardar**.
8. En la tabla de la aplicación, haga clic en +.
9. En el campo **Server**, especifique el FQDN del servidor de BEMS local.
10. En el campo **Puerto**, especifique el puerto del clúster de BlackBerry Proxy que se utiliza para acceder al servidor. De forma predeterminada, el puerto es el 8443.
11. En la lista desplegable **Priority**, especifique la prioridad de los servidores correspondientes como principales.
12. En el la lista desplegable **Clúster principal de BlackBerry Proxy**, especifique el nombre del clúster de BlackBerry Proxy que desea establecer como el clúster principal.
13. En el la lista desplegable **Clúster secundario de BlackBerry Proxy**, especifique el nombre del clúster de BlackBerry Proxy que desea establecer como el clúster secundario.
14. Haga clic en **Guardar**.
15. Repita los pasos del 5 al 14 para las siguientes aplicaciones:
    - BlackBerry Connect
    - Servicio de BlackBerry Presence

Exportación del certificado de BlackBerry Proxy al equipo local

Si necesita configurar la comunicación SSL para permitir la comunicación entre BlackBerry Connectivity Node y los servicios locales de BEMS (por ejemplo, los servicios de Connect, Docs y Mail), exporte las cadenas de certificado raíz e intermedio de BlackBerry Proxy e impórtelas en el almacén de claves de Java de BEMS y en el almacén de claves de Windows.

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

Antes de empezar: Compruebe que BlackBerry Connectivity Node está instalado y con el estado En ejecución.

1. En el ordenador que aloja BlackBerry Connectivity Node, exporte el certificado de BlackBerry Proxy al equipo. En un navegador, escriba `https://localhost:17433`. Se mostrará un error de certificado porque la CA que firmó el certificado no se reconoce como una entidad de certificación conocida.
2. Para abrir el cuadro de diálogo Certificado, haga clic en el icono de certificado del campo URL.
3. Haga clic en **Certificate** (Certificado).
4. Haga clic en **Certificate Path**.
5. Haga clic en el certificado raíz. El certificado raíz es el primer elemento de la jerarquía de certificados.
6. Haga clic en **Ver certificado**.
7. Haga clic en la pestaña **Detalles**.
8. Haga clic en **Copiar a archivo**.
9. Haga clic en **Siguiente**.
10. Seleccione **Base-64 encoded X.509 (.CER)**.
11. Haga clic en **Siguiente**.
12. Haga clic en **Examinar**.
13. Introduzca un nombre para el certificado (por ejemplo, ca.cer) y expórtelo al equipo local.
14. Haga clic en **Guardar**.
15. Haga clic en **Finalizar**.
16. Haga clic en **Aceptar**.

Después de terminar:

- Si configura el servicio de Connect, copie el certificado de BlackBerry Proxy exportado en el ordenador que aloja BEMS y Importación del certificado al almacén de claves de Windows de BEMS.
- Si configura los servicios de Presence y Docs, copie el certificado de BlackBerry Proxy exportado en el ordenador que aloja BEMS y Importación del certificado en el almacén de claves de Java en BEMS.

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 BlackBerry UEM.

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

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

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

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

Requisito previo	Detalles
Iniciar sesión	Inicie sesión en BlackBerry UEM como administrador de seguridad. Solo un administrador debe realizar actividades de migración en un momento dado.
Comprobación de la versión de software	Para migrar los datos a BlackBerry UEM Cloud, la instancia de BlackBerry UEM local desde la que se van a migrar los datos debe corresponderse con BlackBerry UEM versión 12.13 o posterior.
BlackBerry Connectivity Node	Para utilizar todas las funciones de migración, active al menos una instancia de BlackBerry Connectivity Node que ejecute la versión 2.13 o posterior.

Requisito previo	Detalles
Configuración de la conexión con el directorio de la empresa de BlackBerry UEM	Configure la conexión con el directorio de la empresa de BlackBerry UEM de destino de la misma forma en que está configurada en el origen. Por ejemplo, si el origen se ha configurado para la integración de Active Directory y se ha conectado al dominio ejemplo.com, configure BlackBerry UEM de destino para la integración de Active Directory y conéctelo al dominio ejemplo.com. **Importante:** La migración no funciona si el directorio de la empresa del servidor de destino no coincide con el directorio de la empresa del servidor de origen.
BlackBerry UEM Client	BlackBerry UEM Client debe tener el SDK de BlackBerry Dynamics versión 8.0 o posterior. Puede encontrar la versión de SDK en las notas de la versión de la aplicación.
Comprobación del estado de las aplicaciones de BlackBerry Dynamics	Compruebe la versión del SDK de BlackBerry Dynamics de todas las aplicaciones de BlackBerry Dynamics que desea migrar. Esto incluye las aplicaciones propias, las aplicaciones de BlackBerry Dynamics, las aplicaciones ISV de terceros y las aplicaciones personalizadas internas. Para las migraciones desde una base de datos de origen de BlackBerry UEM local, todas las aplicaciones de BlackBerry Dynamics deben tener la versión de SDK de BlackBerry Dynamics 8.0 o posterior. Puede encontrar la versión de SDK en las notas de la versión de la aplicación. **Las aplicaciones de BlackBerry Dynamics que no sean compatibles con la migración se borrarán del dispositivo cuando el administrador inicie la migración.**
Comprobación de las autorizaciones de las aplicaciones de BlackBerry Dynamics	Asegúrese de que: • La instancia de BlackBerry UEM de destino tiene la misma lista de autorizaciones de aplicaciones de BlackBerry Dynamics que el servidor de origen. • A todas las cuentas de usuario migradas se les asigna la misma lista de autorizaciones de aplicaciones de BlackBerry Dynamics que la instancia de BlackBerry UEM de destino tiene en el servidor de origen. • La delegada de autenticación es la mismo en el servidor de origen y de destino. Puede cambiar la delegada de autenticación después de la migración. • El perfil de BlackBerry Dynamics del usuario permite que BlackBerry Dynamics active la instancia de BlackBerry UEM Client si la instancia de BlackBerry UEM Client del usuario que se encuentra en el servidor de origen también lo activa BlackBerry Dynamics.  **PRECAUCIÓN:** Si faltan autorizaciones, las aplicaciones de BlackBerry Dynamics se desactivarán después de la migración.
Revisión de ID de empresa	Las aplicaciones personalizadas solo se migran si los servidores de origen y destino tienen el mismo ID de empresa. Es posible combinar dos organizaciones. Para obtener más información, visite support.blackberry.com/community para leer el artículo 47626.

Requisito previo	Detalles
Comprobación de que los puertos necesarios no están bloqueados por un firewall ni los está utilizando otro software	Asegúrese de que el puerto 8887 (TCP) está abierto entre el servidor de BlackBerry UEM local y BlackBerry Connectivity Node. El servidor local escucha en el puerto 8887 para buscar las conexiones del BlackBerry Connectivity Node. Asegúrese de que el puerto que utiliza la instancia de Microsoft SQL Server que aloja la base de datos de BlackBerry UEM local está abierto y se puede acceder a él mediante BlackBerry Connectivity Node (por ejemplo, el puerto 1433).

Conexión con un servidor de origen

Debe conectar BlackBerry UEM al servidor de origen desde el que va a migrar los datos.

Nota: Si hay más de un BlackBerry Connectivity Node activado, asegúrese de configurar todas las instancias de BlackBerry Connectivity Node para que se conecten a la misma base de datos de origen. Todos los BlackBerry Connectivity Node s deben estar ejecutándose.

Nota: Para conectarse a un servidor de origen diferente al que está configurado, elimine la configuración de origen existente y, a continuación, agregue la nueva.

1. En la barra de menús de la consola de gestión de BlackBerry Connectivity Node, haga clic en **Configuración general > Migración**.
2. Haga clic en +.
3. En el campo **Nombre para mostrar**, escriba un nombre descriptivo para la base de datos de origen.
4. En el campo **Servidor de base de datos**, escriba el nombre del equipo que aloja la base de datos de origen; utilice el formato <host>\<instancia> para un puerto dinámico y el formato <host>:<puerto> para un puerto estático.
5. En la lista desplegable **Tipo de autenticación de la base de datos**, seleccione el tipo de autenticación que utiliza para conectarse a la base de datos de origen.
6. Lleve a cabo una de estas acciones:

Opción	Descripción
Si selecciona Autenticación de SQL	a. En los campos **Nombre de usuario de SQL** y **Contraseña de SQL**, escriba su información de inicio de sesión para conectar con la base de datos de origen. b. En el campo **Nombre de la base de datos**, escriba el nombre de la base de datos de origen.
Si selecciona Autenticación de Windows NT	a. Cambie las propiedades de inicio de sesión del servicio BlackBerry UEM - BlackBerry Cloud Connector a la misma cuenta utilizada para instalar el servicio BlackBerry UEM de origen. Para obtener más información sobre el inicio de sesión en cuentas, consulte el artículo Permisos de servicios de Microsoft TechNet. **Nota:** Una vez que se haya completado la migración desde este origen, cambie la configuración de las propiedades de inicio de sesión a la cuenta del sistema local. b. En el campo **Nombre de la base de datos**, escriba el nombre de la base de datos de origen.

7. Haga clic en **Guardar**.
8. En la barra de menús de la consola de gestión de BlackBerry UEM, haga clic en **Configuración > Migración > Configuración**.
9. Haga clic en +.
10. Escriba un nombre descriptivo para la base de datos de origen.
11. Para probar la conexión entre el origen y el destino, haga clic en **Probar conexión**.
12. Haga clic en **Guardar**.

Después de terminar:

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

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

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

- Políticas de TI seleccionadas
- Perfiles de correo electrónico
- Perfiles de Wi-Fi
- Perfiles VPN
- Perfiles de proxy
- Perfiles de 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

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

BlackBerry UEM

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

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

Aplicaciones activadas con BlackBerry Dynamics

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

Elemento	Consideraciones
Perfiles de conectividad	Cuando se migran perfiles de conectividad de BlackBerry Dynamics, los valores de la pestaña Servidores de aplicaciones no se migran. Los valores se rellenan utilizando los valores predeterminados del servidor de destino de BlackBerry UEM. Cuando se migran perfiles de conectividad de BlackBerry Dynamics, algunos valores de la pestaña Infraestructura no se migran. El administrador debe editar manualmente cada perfil migrado y establecer los valores del clúster de BlackBerry Proxy y el clúster de BlackBerry Proxy secundario.
Aplicaciones	Si un derecho de aplicación del servidor de origen no existe en el servidor de destino, la asignación de la aplicación no se migra. El grupo de aplicaciones se migra.
Uso de certificados	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

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

Tras migrar usuarios, dispositivos, grupos y otros datos a BlackBerry UEM, debe completar las siguientes tareas en el BlackBerry UEM de destino.

Para restablecer las relaciones entre aplicaciones, políticas y usuarios:

- Asigne las configuraciones de aplicaciones a aplicaciones de BlackBerry Dynamics en grupos.
- Asigne los perfiles de conectividad a grupos.
- Asigne las políticas de BlackBerry Dynamics migradas a usuarios.
- Configure los perfiles de anulación (perfiles de BlackBerry Dynamics y de conformidad).

Para completar los perfiles de conectividad migrados:

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

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

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

1. En la barra de menús, haga clic en **Configuración**.
2. Haga clic en **Migración** > **Políticas de TI, perfiles, grupos**.
3. Haga clic en **Siguiente**.
4. Seleccione las casillas de verificación de los elementos que desea migrar.
   El nombre del servidor de origen se anexa a cada nombre de perfil y política durante la migración al destino.
5. Haga clic en **Vista previa** para revisar las políticas y los perfiles seleccionados.
6. Haga clic en **Migrar**.
7. Para configurar las políticas de TI, los perfiles y los grupos, haga clic en **Configurar políticas y perfiles de TI** y vaya a la pantalla **Políticas y perfiles**.

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

Consideraciones: Migración de usuarios desde un servidor de origen

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

Elemento	Consideraciones
Número máximo para migrar	Puede migrar un máximo de 1000 usuarios a la vez desde un origen. Si selecciona un número mayor que el número máximo de usuarios, solo el número máximo se migrará a la instancia de BlackBerry UEM de destino. El resto de usuarios se omitirá. Repita el proceso de migración tantas veces como sea necesario para migrar todos los usuarios desde el servidor de origen. **Nota:** Si se agota el tiempo de espera de BlackBerry UEM al migrar 1000 usuarios, intente migrar menos usuarios.

Elemento	Consideraciones
Dirección de correo	• Solo se pueden migrar los usuarios con una dirección de correo electrónico asociada. • No se puede migrar un usuario que ya utilice la misma dirección de correo en la instancia de BlackBerry UEM de destino. Estos usuarios no aparecen en la lista de usuarios que se van a migrar. • Si dos usuarios en la base de datos de origen tienen la misma dirección de correo , solo un usuario se muestra en la pantalla Migrar usuarios.
Contraseña	Después de la migración, los usuarios locales deben cambiar sus contraseñas después de iniciar sesión en BlackBerry UEM Self-Service por primera vez. A los usuarios que no tienen permiso para acceder a BlackBerry UEM Self-Service antes de la migración no se les concede automáticamente el permiso después de la migración.
Grupos	• Puede filtrar los usuarios sin grupo asignado para incluir este conjunto de usuarios para una migración. • No puede migrar un usuario que sea propietario de un grupo de dispositivos compartidos. El usuario no aparece en la lista de usuarios que se van a migrar.

Migración de usuarios desde un servidor de origen

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

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

   La caché tarda aproximadamente 10 minutos en rellenar 1000 usuarios.

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

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

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

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

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

Consideraciones: migración de dispositivos desde un servidor de origen

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

Elemento	Consideraciones
Número máximo para migrar	Puede migrar un máximo de 2000 dispositivos a la vez desde un servidor de origen.
BlackBerry UEM de destino	Antes de migrar los dispositivos, verifique que BlackBerry UEM es compatible con el tipo y el SO del dispositivo.
Usuarios	• Los usuarios deben existir en el dominio de BlackBerry UEM de destino. • Debe migrar todos los dispositivos del usuario al mismo tiempo.
Dispositivos iOS administrados	• Los dispositivos iOS deben tener la versión más reciente de BlackBerry UEM Client instalada. • Los dispositivos iOS asignados al perfil de bloqueo de aplicaciones no se pueden migrar porque BlackBerry UEM Client no puede abrirse para la migración. • En la configuración de la aplicación de todas las aplicaciones relevantes, desactive la casilla de verificación **Eliminar la aplicación del dispositivo cuando este se haya eliminado de BlackBerry UEM**. **Nota:** Si intenta realizar la migración sin realizar este paso, la aplicación se eliminará y el dispositivo podría desinscribirse de BlackBerry UEM. Sin embargo, incluso si desactiva esta casilla de verificación, la aplicación se puede eliminar durante la migración si la configuración no se ha enviado al dispositivo. Para obtener más información sobre los comandos de seguimiento que se envían a un dispositivo, visite support.blackberry.com/community para leer el artículo 102688.
Dispositivos Android administrados	• Los dispositivos Android Enterprise deben tener la versión más reciente de BlackBerry UEM Client instalada. • No se pueden migrar los dispositivos Android con un perfil de trabajo que utiliza una cuenta de Google o un dominio de Google.
Dispositivos Windows	No se pueden migrar los dispositivos Windows.
Dispositivos macOS	No se pueden migrar los dispositivos macOS.
Controles de MDM	Los dispositivos activados con "Controles de MDM " pierden temporalmente el acceso al correo cuando la migración comience. Los servicios de correo se restauran cuando se completa la migración.
Grupos	No puede migrar un dispositivo que pertenece a un grupo de dispositivos compartidos. Estos dispositivos no aparecen en la lista de migración.

Elemento	Consideraciones
Dispositivos con BlackBerry Dynamics	**Aplicaciones de BlackBerry Dynamics** • Se han migrado todas las aplicaciones de BlackBerry Dynamics compatibles con la migración. **Las aplicaciones de BlackBerry Dynamics que no sean compatibles con la migración se borrarán cuando el administrador active la migración.** Estas aplicaciones se deben volver a activar en el BlackBerry UEM de destino. • Para las migraciones desde una base de datos de origen de BlackBerry UEM local, todas las aplicaciones de BlackBerry Dynamics deben tener la versión de SDK de BlackBerry Dynamics 8.0 o posterior. • En la pantalla Migrar dispositivos, la columna Contenedores incompatibles muestra el número de aplicaciones de BlackBerry Dynamics de cada dispositivo que no se pueden migrar y el número total de aplicaciones de BlackBerry Dynamics de cada dispositivo. Haga clic en el número para ver las aplicaciones de BlackBerry Dynamics que son incompatibles con la migración. • Asegúrese de que el usuario tiene las autorizaciones de la aplicación en el BlackBerry UEM de destino. Si la aplicación no tiene el derecho, después de la migración, el usuario recibirá un mensaje que indica que la aplicación está bloqueada. • Las aplicaciones de BlackBerry Dynamics no se migran si el BlackBerry UEM de destino ya tiene aplicaciones registradas para ese usuario. • BlackBerry Access for Windows, BlackBerry Access for macOS y BlackBerry Enterprise BRIDGE no son compatibles con la migración. Cuando haya finalizado la migración, los usuarios tendrán que volver a inscribir estas aplicaciones en UEM. • Las aplicaciones personalizadas solo se migran si los servidores de origen y destino tienen el mismo ID de empresa. Es posible combinar dos organizaciones. Para obtener más información, visite support.blackberry.com/community para leer el artículo 47626. • Los dispositivos con aplicaciones de BlackBerry Dynamics activadas por varios usuarios no se deben migrar. • Es posible que las aplicaciones de BlackBerry Dynamics bloqueadas debido al cumplimiento o de forma remota por el administrador antes de que tuviese lugar el proceso de migración dejen de funcionar después de la migración y es posible que deban reactivarse. Si BlackBerry UEM Client está bloqueado, el usuario no se puede migrar. • El proceso de migración no realiza un seguimiento ni garantiza la migración de BlackBerry UEM Client ni de las aplicaciones activadas en un dispositivo después de que los datos del dispositivo se hayan almacenado en caché. Los administradores deben actualizar la caché del usuario antes de cada migración. **Autenticación de dispositivos** • El delegado de autenticación debe ser el mismo en el servidor de origen y la instancia de BlackBerry UEM de destino. Puede cambiar la delegada de autenticación después de la migración.

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

Migración de dispositivos desde un servidor de origen

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

Antes de empezar:

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

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

   La caché tarda aproximadamente 10 minutos en rellenar 1000 dispositivos.

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

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

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

   Si se han realizado cambios en el origen una vez actualizada la caché, dichos cambios no se reflejarán en los datos de caché mostrados. No debería realizar cambios en el servidor de origen durante la migración, pero si los realiza, actualice la caché periódicamente.
5. Haga clic en **Vista previa**.
6. Haga clic en **Migrar**.
7. Para ver el estado de los dispositivos que se van a migrar, haga clic en **Migración** > **Estado**.

Referencia rápida de migración de dispositivos

Tipo de dispositivo	Configuración/tipo de activación	Migración
Android	• Controles de MDM • BlackBerry 2FA • Privacidad del usuario • BlackBerry Dynamics (UEM a UEM)	Compatibilidad
Los dispositivos con Android Enterprise que tienen un perfil de trabajo asociado con un dominio de Google	Cualquiera	No es compatible

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

Migración de dispositivos DEP

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

Nota: La configuración de inscripción de DEP no se migra y los dispositivos perderán la configuración de inscripción en el entorno de destino. Para obtener más información, visite support.blackberry.com y lea el artículo KB 100525.

Migración de dispositivos DEP que tienen BlackBerry UEM Client instalado

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

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

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

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

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

Después de terminar:

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

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

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

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

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

Aviso legal

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

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

EXCEPTO EN LA MEDIDA EN QUE LO PROHÍBA ESPECÍFICAMENTE LA LEY DE SU JURISDICCIÓN, QUEDAN EXCLUIDAS POR LA PRESENTE TODAS LAS CONDICIONES, APROBACIONES O GARANTÍAS DE CUALQUIER TIPO, EXPLÍCITAS O IMPLÍCITAS, INCLUIDA, SIN NINGÚN TIPO DE LIMITACIÓN, CUALQUIER CONDICIÓN, APROBACIÓN, GARANTÍA, DECLARACIÓN DE GARANTÍA DE DURABILIDAD, IDONEIDAD PARA UN FIN O USO DETERMINADO, COMERCIABILIDAD, CALIDAD COMERCIAL, ESTADO DE NO INFRACCIÓN, CALIDAD SATISFACTORIA O TITULARIDAD, O QUE SE DERIVE DE UNA LEY O COSTUMBRE O UN CURSO DE LAS NEGOCIACIONES O USO DEL COMERCIO, O RELACIONADO CON LA DOCUMENTACIÓN O SU USO O RENDIMIENTO O NO RENDIMIENTO DE CUALQUIER SOFTWARE, HARDWARE, SERVICIO O CUALQUIER PRODUCTO O SERVICIO DE TERCEROS MENCIONADOS AQUÍ. ASIMISMO, PODRÍA DISPONER DE OTROS DERECHOS QUE VARÍAN SEGÚN EL ESTADO O LA PROVINCIA. ES POSIBLE QUE ALGUNAS JURISDICCIONES NO PERMITAN LA EXCLUSIÓN O LA LIMITACIÓN DE GARANTÍAS Y CONDICIONES IMPLÍCITAS. EN LA MEDIDA EN QUE LO PERMITA LA LEY, CUALQUIER GARANTÍA IMPLÍCITA O CONDICIONES EN RELACIÓN CON LA DOCUMENTACIÓN NO SE PUEDEN EXCLUIR TAL Y COMO SE HA EXPUESTO ANTERIORMENTE, PERO PUEDEN SER LIMITADAS, Y POR LA PRESENTE ESTÁN LIMITADAS A NOVENTA (90) DÍAS DESDE LA FECHA QUE ADQUIRIÓ LA DOCUMENTACIÓN O EL ELEMENTO QUE ES SUJETO DE LA RECLAMACIÓN.

EN LA MEDIDA MÁXIMA EN QUE LO PERMITA LA LEY DE SU JURISDICCIÓN, EN NINGÚN CASO BLACKBERRY ASUMIRÁ RESPONSABILIDAD ALGUNA POR CUALQUIER TIPO DE DAÑOS RELACIONADOS CON ESTA DOCUMENTACIÓN O SU USO, O POR EL RENDIMIENTO O NO RENDIMIENTO DE CUALQUIER SOFTWARE, HARDWARE, SERVICIO O PRODUCTOS Y SERVICIOS DE TERCEROS AQUÍ MENCIONADOS INCLUIDOS SIN NINGÚN TIPO DE LIMITACIÓN CUALQUIERA DE LOS SIGUIENTES DAÑOS: DIRECTOS, RESULTANTES, EJEMPLARES, INCIDENTALES, INDIRECTOS, ESPECIALES, PUNITIVOS O AGRAVADOS, DAÑOS POR PÉRDIDA DE BENEFICIOS O INGRESOS, IMPOSIBILIDAD DE CONSEGUIR LOS AHORROS ESPERADOS, INTERRUPCIÓN DE LA ACTIVIDAD COMERCIAL, PÉRDIDA DE INFORMACIÓN COMERCIAL, PÉRDIDA DE LA OPORTUNIDAD DE NEGOCIO O DAÑO O PÉRDIDA DE DATOS, IMPOSIBILIDAD DE TRANSMITIR O RECIBIR CUALQUIER DATO, PROBLEMAS ASOCIADOS CON CUALQUIER APLICACIÓN QUE SE UTILICE JUNTO CON PRODUCTOS Y SERVICIOS DE BLACKBERRY, COSTES DEBIDOS AL TIEMPO DE INACTIVIDAD, PÉRDIDA DE USO DE LOS PRODUCTOS Y

SERVICIOS DE BLACKBERRY O PARTE DE ELLOS O DE CUALQUIER SERVICIO DE USO, COSTE DE SERVICIOS SUSTITUTIVOS, COSTES DE COBERTURA, INSTALACIONES O SERVICIOS, COSTE DEL CAPITAL O CUALQUIER OTRA PÉRDIDA MONETARIA SIMILAR, TANTO SI DICHOS DAÑOS SE HAN PREVISTO COMO SI NO, Y AUNQUE SE HAYA AVISADO A BLACKBERRY DE LA POSIBILIDAD DE DICHOS DAÑOS.

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

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

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

Antes de instalar, usar o suscribirse a cualquiera de los Productos y servicios de terceros, es su responsabilidad asegurarse de que su proveedor de servicios de uso ofrezca compatibilidad con todas sus funciones. Es posible que algunos proveedores de servicios de uso no ofrezcan la función de exploración de Internet con una suscripción a BlackBerry® Internet Service. Consulte con su proveedor de servicios acerca de la disponibilidad, arreglos de itinerancia, planes de servicio y funciones. La instalación o el uso de Productos y servicios de terceros con productos y servicios de BlackBerry pueden precisar la obtención de una o más patentes, marcas comerciales, derechos de autor u otras licencias para evitar que se vulneren o infrinjan derechos de terceros. Usted es el único responsable de determinar si desea utilizar Productos y servicios de terceros y si se necesita para ello cualquier otra licencia de terceros. En caso de necesitarlas, usted es el único responsable de su adquisición. No instale o utilice Productos y servicios de terceros hasta que se hayan adquirido todas las licencias necesarias. Cualquier tipo de Productos y servicios de terceros que se proporcione con los productos y servicios de BlackBerry se le facilita para su comodidad "TAL CUAL" sin ninguna condición expresa e implícita, aprobación, garantía de cualquier tipo por BlackBerry, y BlackBerry no asume ninguna responsabilidad en relación con ellos. El uso de los Productos y servicios de terceros estará sujeto a la aceptación de los términos de las licencias independientes aplicables en este caso con terceros, excepto en los casos cubiertos expresamente por una licencia u otro acuerdo con BlackBerry.

Los términos de uso de cualquier producto o servicio de BlackBerry se presentan en una licencia independiente o en otro acuerdo con BlackBerry aplicable según corresponda. NADA DE LO DISPUESTO EN LA PRESENTE DOCUMENTACIÓN SUSTITUIRÁ NINGÚN ACUERDO EXPRESO POR ESCRITO NI NINGUNA GARANTÍA QUE PROPORCIONE BLACKBERRY PARA PARTES DE CUALQUIER PRODUCTO O SERVICIO DE BLACKBERRY QUE NO SEA ESTA DOCUMENTACIÓN.

BlackBerry Enterprise Software incluye software de terceros. La información de licencia y copyright asociada a este software está disponible en http://worldwide.blackberry.com/legal/thirdpartysoftware.jsp.

BlackBerry Limited
2200 University Avenue East
Waterloo, Ontario
Canadá N2K 0A7

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

Publicado en Canadá