BlackBerry UEM

Arquitectura y flujos de datos

12.17

Contents

Arquitectura y flujos de datos de BlackBerry UEM..... 5
Arquitectura: solución BlackBerry UEM..... 5

Componentes de BlackBerry UEM..... 8

Instalación distribuida de BlackBerry UEM..... 11

Implementación regional de BlackBerry UEM..... 15

Activación de dispositivos y de las aplicaciones de BlackBerry Dynamics..... 18
Flujo de datos: activación de un dispositivo con Android Enterprise Trabajo y personal: privacidad de usuario mediante una cuenta de Google Play gestionada..... 18
Flujo de datos: activación de un dispositivo Android Enterprise Trabajo y personal: control total mediante una cuenta de Google Play gestionada..... 20
Flujo de datos: activación de un dispositivo Android Enterprise Solo espacio de trabajo mediante una cuenta de Google Play gestionada..... 21
Flujo de datos: activación de un dispositivo Android Enterprise Trabajo y personal: privacidad de usuario en un dominio de Google..... 23
Flujo de datos: activación de un dispositivo Android Enterprise Trabajo y personal: control total en un dominio de Google..... 24
Flujo de datos: activación de un dispositivo Android Enterprise Solo espacio de trabajo en un dominio de Google..... 26
Flujo de datos: activación de un dispositivo para que utilice Knox Workspace..... 28
Flujo de datos: activación de un dispositivo iOS..... 29
Flujo de datos: activación de un dispositivo macOS..... 32
Flujo de datos: activación de un dispositivo Windows 10..... 33
Flujo de datos: activación de una aplicación de BlackBerry Dynamics por primera vez en un dispositivo..... 35
Flujo de datos: activación de una aplicación de BlackBerry Dynamics cuando ya hay una activada en el dispositivo..... 36

Envío y recepción de datos de trabajo..... 37
Envío y recepción de datos de trabajo mediante BlackBerry Infrastructure..... 38
Flujo de datos: envío y recepción de datos de trabajo desde una aplicación de BlackBerry Dynamics mediante BlackBerry Dynamics NOC..... 39
Flujo de datos: envío y recepción de datos de trabajo desde una aplicación de BlackBerry Dynamics mediante BlackBerry Infrastructure..... 40
Flujo de datos: envío y recepción de datos de trabajo desde una aplicación de BlackBerry Dynamics mediante BlackBerry Dynamics Direct Connect..... 40
Flujo de datos: acceso a un servidor de aplicaciones o contenido mediante BlackBerry Secure Connect Plus..... 41

Flujo de datos: envío y recepción de datos de trabajo desde una aplicación de BlackBerry Dynamics en un dispositivo Android utilizando BlackBerry Secure Connect Plus....42
Flujo de datos: autenticación con el servidor de correo desde un dispositivo con iOS cuando se usa BlackBerry Secure Gateway....43
Flujo de datos: envío de correo desde un dispositivo iOS con BlackBerry Secure Gateway.... 44
Flujo de datos: recepción de correo en un dispositivo iOS con BlackBerry Secure Gateway....44
Envío y recepción de datos de trabajo mediante una VPN o red Wi-Fi de trabajo....46
Flujo de datos: envío de correo desde un dispositivo mediante una red VPN o una red Wi-Fi de trabajo....46
Flujo de datos: recepción de correo en un dispositivo mediante una red VPN o una red Wi-Fi de trabajo....47
Flujo de datos: acceso a un servidor de aplicaciones o de contenido mediante una red VPN o una red Wi-Fi de trabajo.... 48

Recepción de actualizaciones de configuración del dispositivo....49
Flujo de datos: recepción de actualizaciones de configuración en un dispositivo Android.... 50
Flujo de datos: actualización del firmware en dispositivos Samsung Knox....51
Flujo de datos: recepción de actualizaciones de configuración en un dispositivo iOS.... 52
Flujo de datos: recepción de actualizaciones de configuración en un dispositivo macOS.... 53
Flujo de datos: recepción de actualizaciones de configuración en un dispositivo Windows 10....53

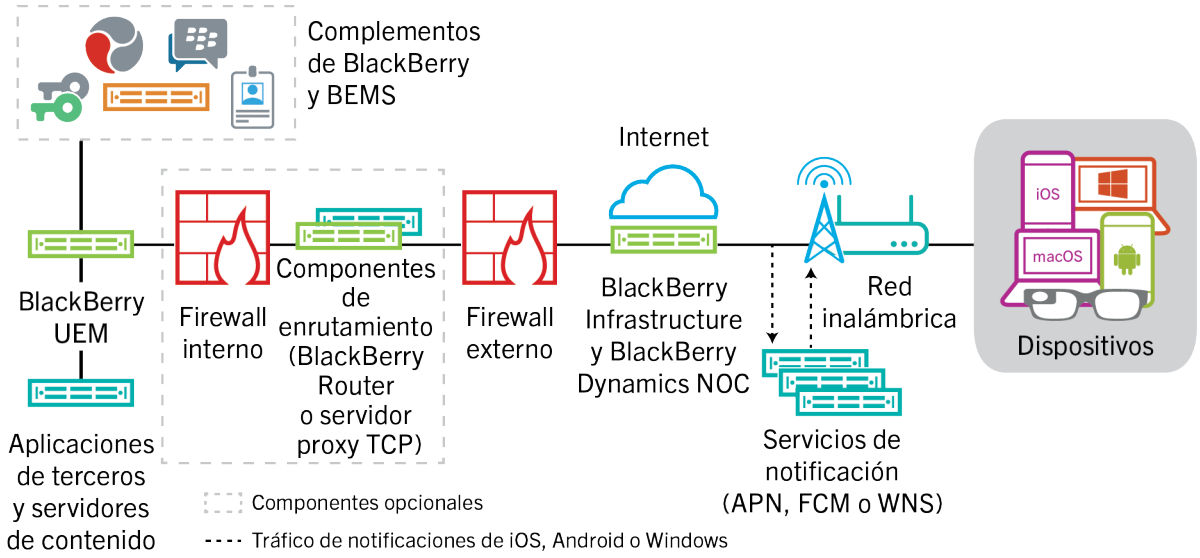
Aviso legal.... 55

Arquitectura y flujos de datos de BlackBerry UEM

BlackBerry UEM es una solución EMM multiplataforma de BlackBerry que proporciona una administración completa de dispositivos, aplicaciones y contenidos con seguridad y conectividad integradas, y que le ayuda a administrar los dispositivos iOS, macOS, Android, Windows 10 y para su empresa.

La arquitectura de BlackBerry UEM se ha diseñado para ayudarle a administrar los dispositivos móviles de su empresa y proporcionar un enlace seguro para los datos que se desplazan entre los servidores de correo y contenido de su empresa y los dispositivos de sus usuarios.

Arquitectura: solución BlackBerry UEM



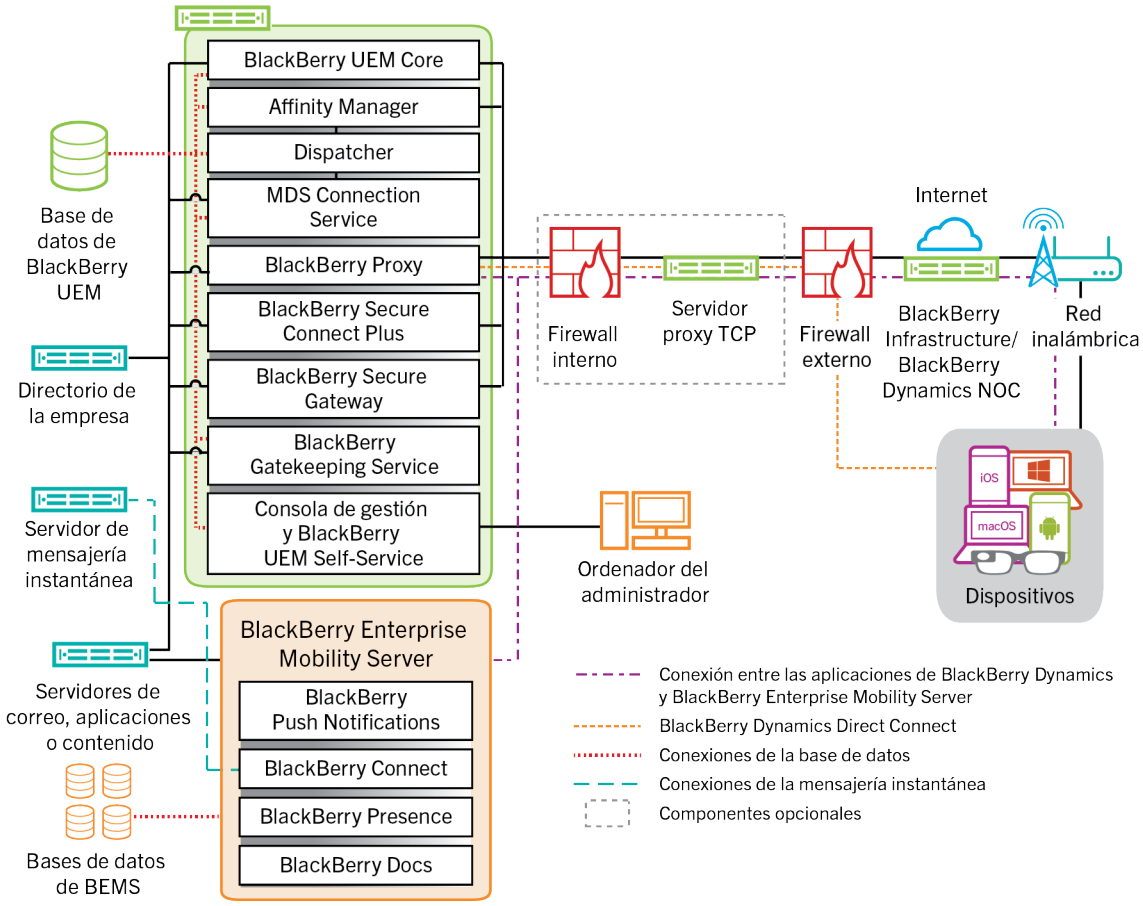
Componente	Descripción
BlackBerry UEM	BlackBerry UEM es una solución de gestión unificada de extremos que ofrece una gestión exhaustiva multiplataforma de dispositivos, aplicaciones y contenido con seguridad y conectividad integradas.

Componente	Descripción
BlackBerry Infrastructure	BlackBerry Infrastructure es una red de datos global privada y distribuida en diferentes regiones que habilita y garantiza la seguridad de los datos en tránsito entre cientos de organizaciones y millones de usuarios de todo el mundo. Esta herramienta ha sido diseñada para administrar el transporte de datos entre los servicios BlackBerry y los dispositivos de los usuarios finales. Para empresas que utilizan BlackBerry UEM, BlackBerry Infrastructure registra la información del usuario para la activación de dispositivos, valida la información de licencias para BlackBerry UEM y proporciona una ruta de confianza entre la empresa y cada usuario basada en una autenticación mutua, sólida y cifrada. Debido al cifrado integral que protege los datos que se transmiten entre el dispositivo y BlackBerry UEM, BlackBerry UEM mantiene una conexión constante a BlackBerry Infrastructure. Esto garantiza que las empresas requieran solo una conexión saliente a una dirección IP de confianza para enviar datos a los usuarios. Todos los datos que se transmiten entre BlackBerry Infrastructure y BlackBerry UEM están autenticados y cifrados para proporcionar un canal de comunicación seguro dentro de la empresa para aquellos dispositivos que se encuentran fuera del firewall.
BlackBerry Dynamics NOC	BlackBerry Dynamics NOC es un centro de operaciones de red que proporciona comunicaciones seguras entre las aplicaciones de BlackBerry Dynamics en los dispositivos, BlackBerry UEM y BlackBerry Enterprise Mobility Server.
Dispositivos	BlackBerry UEM es compatible con dispositivos iOS, macOS, Android y Windows 10.
Servicios de notificación	BlackBerry UEM envía notificaciones a los dispositivos para que se pongan en contacto con BlackBerry UEM para obtener actualizaciones y proporcionar información para el inventario de dispositivos de la empresa. Estas notificaciones se envían a BlackBerry Infrastructure, desde donde se envían al dispositivo a través del servicio de notificación apropiado: • APN es un servicio que proporciona Apple para enviar notificaciones a los dispositivos iOS y macOS. • FCM es un servicio que proporciona Google para enviar notificaciones a los dispositivos con Android. • El servicio de notificación de inserción de Windows (WNS) que proporciona Microsoft para enviar notificaciones a los dispositivos Windows.

Componente	Descripción
Componentes de enrutamiento	De forma predeterminada, BlackBerry UEM establece una conexión directa con BlackBerry Infrastructure a través de los puertos 3101 y 443, por lo que no necesitará instalar más componentes de enrutamiento. No obstante, si la política de seguridad de la empresa requiere que los sistemas internos no puedan establecer conexiones directas a Internet, puede usar BlackBerry Router o un servidor proxy. BlackBerry Router actúa como un servidor proxy para conexiones a través de BlackBerry Infrastructure entre BlackBerry UEM y todos los dispositivos. BlackBerry Router proporciona compatibilidad con SOCKs v5 sin autenticación. Si su empresa ya tiene instalado un servidor proxy TCP o bien necesita uno para cumplir con los requisitos de red, puede utilizar un servidor proxy TCP en lugar de BlackBerry Router. El servidor proxy TCP proporciona compatibilidad con SOCKS v5 sin autenticación. BlackBerry UEM Core y BlackBerry Proxy son compatibles con el uso de un servidor proxy HTTP para conectarse a BlackBerry Dynamics NOC.
Aplicaciones de terceros y servidores de contenido	Servidores de contenido o servidores de aplicaciones adicionales del entorno de la empresa, incluidos el directorio de la empresa, el servidor de correo, las autoridades de certificación, etc.
Complementos de BlackBerry y BEMS	BlackBerry UEM funciona con productos de empresa adicionales de BlackBerry como: BlackBerry Enterprise Identity y BlackBerry 2FA, que le permiten ampliar las capacidades de UEM en su empresa. BlackBerry Enterprise Mobility Server proporciona varios servicios utilizados para enviar datos de trabajo hacia y desde las aplicaciones de BlackBerry Dynamics.

Componentes de BlackBerry UEM

Este diagrama muestra cómo se conectan los componentes de BlackBerry UEM cuando todos los componentes se instalan juntos en la configuración más simple del producto.



Para obtener más información acerca de los puertos utilizados para las conexiones entre los componentes, consulte el contenido de planificación.

Nombre del componente	Descripción
BlackBerry UEM Core	BlackBerry UEM Core es el componente central de la arquitectura de BlackBerry UEM. Está constituido por varios subcomponentes que se encargan de: • Registro, supervisión, presentación de informes y funciones de administración • Los servicios de autenticación y autorización • Programación y envío de comandos, políticas de TI y perfiles a los dispositivos • Envío de datos de usuarios, de la política y otros datos de configuración a las aplicaciones de BlackBerry Dynamics en los dispositivos.
Base de datos de BlackBerry UEM	La base de datos de BlackBerry UEM es una base de datos relacional que contiene información de la cuenta de usuario y la información de configuración que BlackBerry UEM utiliza para administrar dispositivos y aplicaciones de BlackBerry Dynamics.

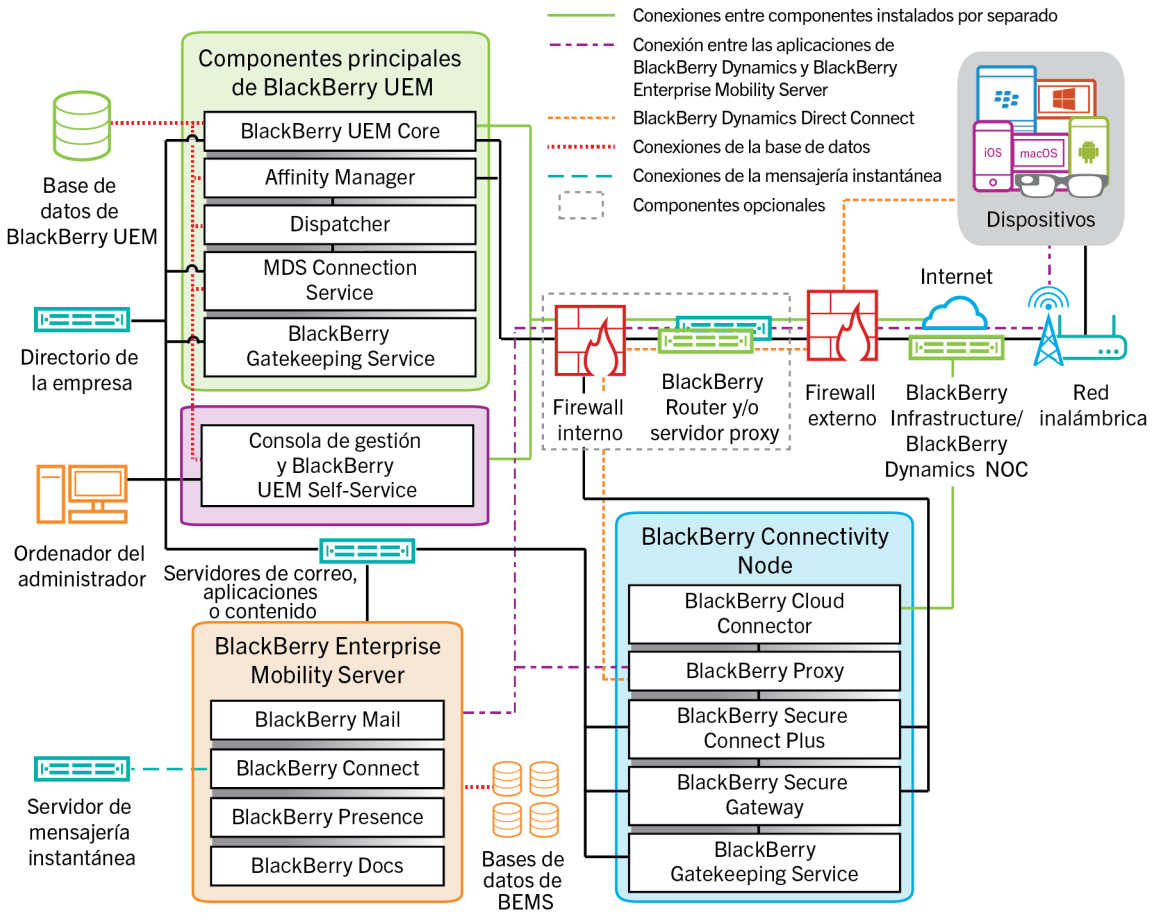
Nombre del componente	Descripción
BlackBerry Proxy	BlackBerry Proxy mantiene la seguridad de la conexión entre su empresa y BlackBerry Dynamics NOC. También admite BlackBerry Dynamics Direct Connect, que permite que los datos de aplicaciones omitan BlackBerry Dynamics NOC.
BlackBerry Secure Connect Plus	BlackBerry Secure Connect Plus proporciona un túnel IP seguro entre las aplicaciones de trabajo en los dispositivos y la red de la empresa. Se establece un túnel que es compatible con datos IPv4 (TCP y UDP) estándar para cada uno de los dispositivos a través de BlackBerry Infrastructure.
BlackBerry Secure Gateway	BlackBerry Secure Gateway proporciona una conexión segura a través de BlackBerry Infrastructure y BlackBerry UEM al servidor de correo de su empresa para dispositivos iOS.
BlackBerry Gatekeeping Service	BlackBerry Gatekeeping Service envía los comandos a Exchange ActiveSync para agregar dispositivos a una lista de dispositivos admitidos cuando los dispositivos están activados en BlackBerry UEM. Los dispositivos no administrados que intentan conectarse a un servidor de correo de la empresa pueden ser revisados, verificados, así como bloqueados o admitidos por un administrador a través de la consola de administración de BlackBerry UEM.
Consola de gestión y BlackBerry UEM Self-Service	La consola de gestión y BlackBerry UEM Self-Service proporcionan una interfaz de usuario basada en web para que el usuario y el administrador accedan a BlackBerry UEM. Puede usar esta consola para gestionar la configuración del sistema, los usuarios, los dispositivos y las aplicaciones. Los usuarios pueden usar BlackBerry UEM Self-Service para establecer una contraseña de activación y enviar comandos a los dispositivos tales como configurar contraseña, bloquear el dispositivo y eliminar los datos de los dispositivos.
BlackBerry Enterprise Mobility Server	BEMS consolida varios servicios utilizados para enviar datos de trabajo hacia y desde las aplicaciones de BlackBerry Dynamics, incluidas: BlackBerry Push Notifications, BlackBerry Connect, BlackBerry Presence y BlackBerry Docs.
Bases de datos BlackBerry Enterprise Mobility Server	Las bases de datos de BEMS guardan la información de los usuarios, aplicaciones, políticas y configuraciones.
BlackBerry Push Notifications	BlackBerry Push Notifications acepta solicitudes de registro de inserción de dispositivos iOS y Android. A continuación, se comunica con Microsoft Exchange para supervisar si se producen cambios en la cuenta de correo de trabajo del usuario.
BlackBerry Connect	BlackBerry Connect proporciona mensajería instantánea, búsqueda en directorios empresariales e información de presencia de usuarios a dispositivos iOS y Android de forma segura.
BlackBerry Presence	BlackBerry Presence proporciona estado de presencia en tiempo real a aplicaciones de BlackBerry Dynamics.

Nombre del componente	Descripción
BlackBerry Docs	BlackBerry Docs permite que los usuarios de aplicaciones de BlackBerry Dynamics accedan, sincronicen y compartan documentos con su servidor de archivos de trabajo, SharePoint, Box y sistemas de gestión de contenido que son compatibles con CMIS, sin necesidad de software de VPN, reconfiguración del firewall o almacenes de datos duplicados.
Servidores proxy o BlackBerry Router	De forma predeterminada, BlackBerry UEM establece una conexión directa con BlackBerry Infrastructure a través de los puertos 3101 y 443. Si la política de seguridad de la empresa requiere que los sistemas internos no puedan conectarse directamente a Internet, puede instalar BlackBerry Router o usar un servidor proxy TCP de terceros que sea compatible con SOCKs v5 sin autenticación. BlackBerry UEM Core y BlackBerry Proxy son compatibles con el uso de un servidor proxy HTTP de terceros para conectarse a BlackBerry Dynamics NOC.
BlackBerry Infrastructure y BlackBerry Dynamics NOC	BlackBerry Infrastructure registra la información del usuario para la activación de dispositivos, valida la información de licencias para BlackBerry UEM y proporciona una ruta de confianza entre la empresa y cada usuario basada en una autenticación mutua, sólida y cifrada. BlackBerry Dynamics NOC es un NOC con ubicación independiente que ofrece comunicaciones seguras entre las aplicaciones de BlackBerry Dynamics en dispositivos y BlackBerry UEM Core, BlackBerry Proxy y BlackBerry Enterprise Mobility Server.

Instalación distribuida de BlackBerry UEM

En este diagrama se muestra cómo los componentes de BlackBerry UEM se interconectan cuando BlackBerry Connectivity Node y la interfaz de usuario están instalados aparte de los componentes principales de BlackBerry UEM.

Para obtener más información sobre la arquitectura cuando se instala BlackBerry UEM en más de un equipo para alta disponibilidad, consulte la Guía de planificación.



Para obtener más información acerca de los puertos utilizados para las conexiones entre los componentes, consulte el contenido de planificación.

Nombre del componente	Descripción
Componentes primarios de BlackBerry UEM	Los componentes de BlackBerry UEM principales incluyen BlackBerry UEM Core y los instalados en el mismo servidor.

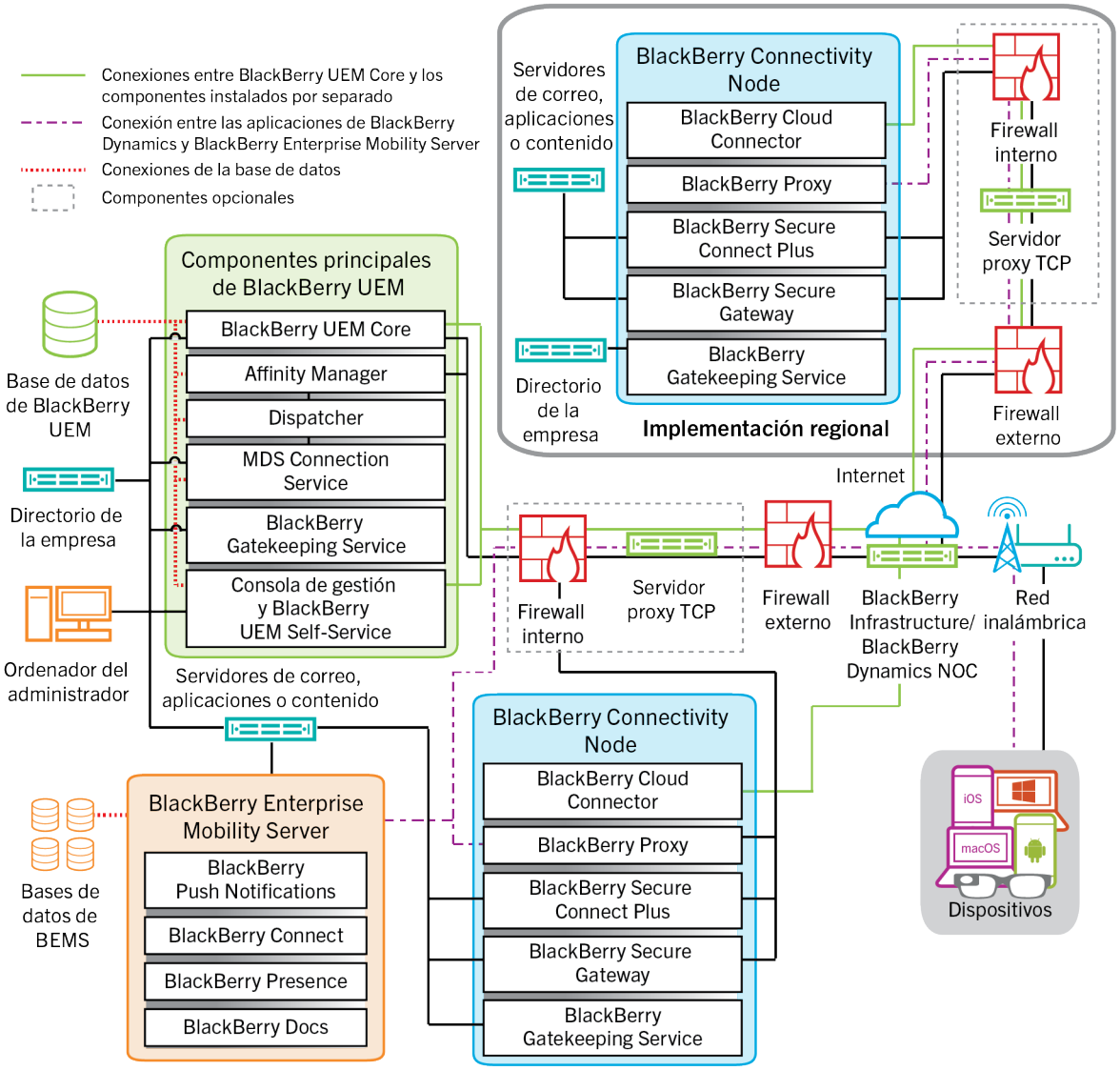
Nombre del componente	Descripción
BlackBerry UEM Core	BlackBerry UEM Core es el componente central de la arquitectura de BlackBerry UEM. Está constituido por varios subcomponentes que se encargan de: • Registro, supervisión, presentación de informes y funciones de administración • Los servicios de autenticación y autorización • Programación y envío de comandos, políticas de TI y perfiles a los dispositivos • Envío de datos de usuarios, de la política y otros datos de configuración a las aplicaciones de BlackBerry Dynamics en los dispositivos.
Base de datos de BlackBerry UEM	La base de datos de BlackBerry UEM es una base de datos relacional que contiene información de la cuenta de usuario y la información de configuración que BlackBerry UEM utiliza para administrar dispositivos y aplicaciones de BlackBerry Dynamics.
BlackBerry Gatekeeping Service (primaria)	BlackBerry Gatekeeping Service envía los comandos a Exchange ActiveSync para agregar dispositivos a una lista de dispositivos admitidos cuando los dispositivos están activados en BlackBerry UEM. Los dispositivos no administrados que intentan conectarse a un servidor de correo de la empresa pueden ser revisados, verificados, así como bloqueados o admitidos a través de la consola de administración de BlackBerry UEM por un administrador.
Componentes de la interfaz de usuario remotos	La consola de administración y BlackBerry UEM Self-Service se pueden instalar por separado desde otros componentes de BlackBerry UEM. Si los instala por separado, también se instalará una instancia de BlackBerry Management Console Core.
BlackBerry Management Console Core	Si está instalado, BlackBerry Management Console Core solo procesa las solicitudes de la interfaz de usuario de la consola de administración y BlackBerry UEM Self-Service. Esto garantiza que estas interfaces responden incluso cuando la carga en BlackBerry UEM Core es alta.
Consola de gestión y BlackBerry UEM Self-Service	La consola de gestión y BlackBerry UEM Self-Service proporcionan una interfaz de usuario basada en web para que el usuario y el administrador accedan a BlackBerry UEM. Se puede instalar por separado desde otros componentes de BlackBerry UEM. Puede usar esta consola para gestionar la configuración del sistema, los usuarios, los dispositivos y las aplicaciones. Los usuarios pueden acceder a BlackBerry UEM Self-Service para establecer una contraseña de activación y enviar comandos tales como establecer contraseña, bloquear el dispositivo y eliminar datos del dispositivo en sus dispositivos.

Nombre del componente	Descripción
BlackBerry Connectivity Node	BlackBerry Connectivity Node instala instancias de los componentes de conectividad del dispositivo BlackBerry UEM en el dominio de su empresa en un servidor diferente de BlackBerry UEM Core. Cada BlackBerry Connectivity Node contiene los componentes siguientes: • BlackBerry Cloud Connector • BlackBerry Proxy • BlackBerry Secure Connect Plus • BlackBerry Secure Gateway • BlackBerry Gatekeeping Service
BlackBerry Cloud Connector	BlackBerry Cloud Connector permite que los componentes de BlackBerry Connectivity Node se comuniquen con BlackBerry UEM Core. La comunicación entre BlackBerry Cloud Connector y BlackBerry UEM Core se realiza a través de BlackBerry Infrastructure.
BlackBerry Proxy	BlackBerry Proxy mantiene la seguridad de la conexión entre su empresa y BlackBerry Dynamics NOC. También admite BlackBerry Dynamics Direct Connect, que permite que los datos de aplicaciones omitan BlackBerry Dynamics NOC.
BlackBerry Secure Connect Plus	BlackBerry Secure Connect Plus proporciona un túnel IP seguro entre las aplicaciones de trabajo en los dispositivos y la red de la empresa. Se establece un túnel que es compatible con datos IPv4 (TCP y UDP) estándar para cada uno de los dispositivos a través de BlackBerry Infrastructure.
BlackBerry Secure Gateway	BlackBerry Secure Gateway proporciona una conexión segura a través de BlackBerry Infrastructure y BlackBerry UEM al servidor de correo de su empresa para dispositivos iOS.
BlackBerry Gatekeeping Service (BlackBerry Connectivity Node)	BlackBerry UEM puede utilizar instancias de BlackBerry Gatekeeping Service que están instaladas con BlackBerry Connectivity Node para gestionar el enlace para su servidor de correo. Cada instancia debe poder acceder al servidor de enlace de su empresa. Si desea que BlackBerry Gatekeeping Service, que se ha instalado con los componentes principales de BlackBerry UEM, gestione los datos de enlace, puede desactivar BlackBerry Gatekeeping Service en cada BlackBerry Connectivity Node.
BlackBerry Enterprise Mobility Server	BEMS consolida varios servicios utilizados para enviar datos de trabajo hacia y desde las aplicaciones de BlackBerry Dynamics, incluidas: BlackBerry Push Notifications, BlackBerry Connect, BlackBerry Presence y BlackBerry Docs.
Bases de datos BlackBerry Enterprise Mobility Server	Las bases de datos de BEMS guardan la información de los usuarios, aplicaciones, políticas y configuraciones.

Nombre del componente	Descripción
BlackBerry Infrastructure y BlackBerry Dynamics NOC	BlackBerry Infrastructure registra la información del usuario para la activación de dispositivos, valida la información de licencias para BlackBerry UEM y proporciona una ruta de confianza entre la empresa y cada usuario basada en una autenticación mutua, sólida y cifrada. BlackBerry Dynamics NOC es un NOC con ubicación independiente que ofrece comunicaciones seguras entre las aplicaciones de BlackBerry Dynamics en dispositivos y BlackBerry UEM Core, BlackBerry Proxy y BlackBerry Enterprise Mobility Server.

Implementación regional de BlackBerry UEM

Este diagrama muestra cómo se conectan entre sí los componentes de BlackBerry UEM cuando una o más instancias de BlackBerry Connectivity Node se instalan en una ubicación independiente. Puede utilizar grupos de servidores para especificar la instancia regional de BlackBerry Connectivity Node a la que se conecta un dispositivo.



Para obtener información acerca de los puertos utilizados para las conexiones entre los componentes, consulte el contenido de Planificación.

Nombre del componente	Descripción
Componentes primarios de BlackBerry UEM	Los componentes de BlackBerry UEM principales incluyen BlackBerry UEM Core y los instalados en el mismo servidor.

Nombre del componente	Descripción
BlackBerry UEM Core	BlackBerry UEM Core es el componente central de la arquitectura de BlackBerry UEM. Está constituido por varios subcomponentes que se encargan de: • Registro, supervisión, presentación de informes y funciones de administración • Los servicios de autenticación y autorización • Programación y envío de comandos, políticas de TI y perfiles a los dispositivos • Envío de datos de usuarios, de la política y otros datos de configuración a las aplicaciones de BlackBerry Dynamics en los dispositivos.
Base de datos de BlackBerry UEM	La base de datos de BlackBerry UEM es una base de datos relacional que contiene información de la cuenta de usuario y la información de configuración que BlackBerry UEM utiliza para administrar dispositivos y aplicaciones de BlackBerry Dynamics.
BlackBerry Gatekeeping Service (primaria)	BlackBerry Gatekeeping Service envía los comandos a Exchange ActiveSync para agregar dispositivos a una lista de dispositivos admitidos cuando los dispositivos están activados en BlackBerry UEM. Los dispositivos no administrados que intentan conectarse a un servidor de correo de la empresa pueden ser revisados, verificados, así como bloqueados o admitidos a través de la consola de administración de BlackBerry UEM por un administrador.
Consola de gestión y BlackBerry UEM Self-Service	La consola de gestión y BlackBerry UEM Self-Service proporcionan una interfaz de usuario basada en web para que el usuario y el administrador accedan a BlackBerry UEM. Se puede instalar por separado desde otros componentes de BlackBerry UEM. Puede usar esta consola para gestionar la configuración del sistema, los usuarios, los dispositivos y las aplicaciones. Los usuarios pueden acceder a BlackBerry UEM Self-Service para establecer una contraseña de activación y enviar comandos tales como establecer contraseña, bloquear el dispositivo y eliminar datos del dispositivo en sus dispositivos.
BlackBerry Connectivity Node	BlackBerry Connectivity Node instala instancias de los componentes de conectividad del dispositivo BlackBerry UEM en el dominio de su empresa en un servidor diferente de BlackBerry UEM Core. Cada BlackBerry Connectivity Node contiene los componentes siguientes: • BlackBerry Cloud Connector • BlackBerry Proxy • BlackBerry Secure Connect Plus • BlackBerry Secure Gateway • BlackBerry Gatekeeping Service Si tiene implementaciones regionales de BlackBerry Connectivity Node, debe configurar la conexión entre BlackBerry UEM Core y el grupo de servidores que contiene BlackBerry Connectivity Node regional.
BlackBerry Cloud Connector	BlackBerry Cloud Connector permite que los componentes de BlackBerry Connectivity Node se comuniquen con BlackBerry UEM Core. La comunicación entre BlackBerry Cloud Connector y BlackBerry UEM Core se realiza a través de BlackBerry Infrastructure.

Nombre del componente	Descripción
BlackBerry Proxy	BlackBerry Proxy mantiene la seguridad de la conexión entre su empresa y BlackBerry Dynamics NOC. También admite BlackBerry Dynamics Direct Connect, que permite que los datos de aplicaciones omitan BlackBerry Dynamics NOC.
BlackBerry Secure Connect Plus	BlackBerry Secure Connect Plus proporciona un túnel IP seguro entre las aplicaciones de trabajo en los dispositivos y la red de la empresa. Se establece un túnel que es compatible con datos IPv4 (TCP y UDP) estándar para cada uno de los dispositivos a través de BlackBerry Infrastructure.
BlackBerry Secure Gateway	BlackBerry Secure Gateway proporciona una conexión segura a través de BlackBerry Infrastructure y BlackBerry UEM al servidor de correo de su empresa para dispositivos iOS.
BlackBerry Gatekeeping Service (BlackBerry Connectivity Node)	BlackBerry UEM puede utilizar instancias de BlackBerry Gatekeeping Service instaladas con BlackBerry Connectivity Node para gestionar el enlace para su servidor de correo. Cada instancia debe poder acceder al servidor de enlace de su empresa. Si desea que BlackBerry Gatekeeping Service, que se ha instalado con los componentes principales de BlackBerry UEM, gestione los datos de enlace, puede desactivar BlackBerry Gatekeeping Service en cada BlackBerry Connectivity Node.
BlackBerry Enterprise Mobility Server	BEMS consolida varios servicios utilizados para enviar datos de trabajo hacia y desde las aplicaciones de BlackBerry Dynamics, incluidas: BlackBerry Push Notifications, BlackBerry Connect, BlackBerry Presence y BlackBerry Docs.
Bases de datos BlackBerry Enterprise Mobility Server	Las bases de datos de BEMS guardan la información de los usuarios, aplicaciones, políticas y configuraciones.
BlackBerry Infrastructure y BlackBerry Dynamics NOC	BlackBerry Infrastructure registra la información del usuario para la activación de dispositivos, valida la información de licencias para BlackBerry UEM y proporciona una ruta de confianza entre la empresa y cada usuario basada en una autenticación mutua, sólida y cifrada. BlackBerry Dynamics NOC es un NOC con ubicación independiente que ofrece comunicaciones seguras entre las aplicaciones de BlackBerry Dynamics en dispositivos y BlackBerry UEM Core, BlackBerry Proxy y BlackBerry Enterprise Mobility Server.

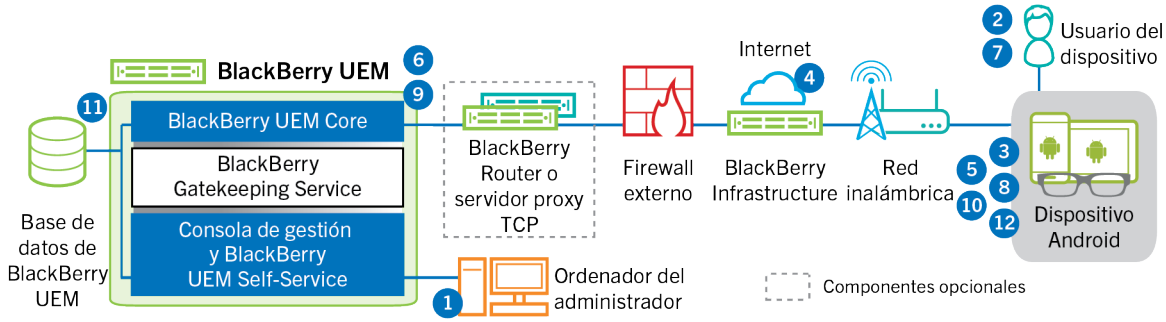
Activación de dispositivos y de las aplicaciones de BlackBerry Dynamics

Cuando un usuario activa un dispositivo con BlackBerry UEM, el dispositivo se asocia con BlackBerry UEM de modo que pueda administrar dispositivos y que los usuarios puedan acceder a los datos de trabajo desde sus dispositivos. Los tipos de activación de dispositivos ofrecen distintos grados de control sobre los datos de trabajo y los datos personales en los dispositivos, que van desde el control total sobre todos los datos al control específico únicamente de los datos de trabajo. Para obtener más información acerca de los tipos de activación, consulte "Activación de dispositivos" en el contenido de Administración.

Dependiendo del tipo de dispositivo y el tipo de activación que especifique, el dispositivo y BlackBerry UEM deben completar varios pasos durante el proceso de activación para que se autentiquen mutuamente, protejan un canal de comunicación y, si es necesario, creen un espacio de trabajo o cifren el dispositivo antes de enviar cualquier configuración y datos de trabajo al dispositivo. Para obtener más información sobre cómo activar dispositivos, consulte "Pasos para activar los dispositivos" en el contenido de Administración.

Las aplicaciones de BlackBerry Dynamics proporcionan acceso a los recursos de trabajo desde el dispositivo. Después de instalar las aplicaciones de BlackBerry Dynamics en un dispositivo, estas también deben activarse para permitir que accedan de forma segura a los recursos de trabajo. Para obtener más información sobre la activación de BlackBerry Dynamics, consulte "Generación de claves de acceso, contraseñas de activación o códigos QR para aplicaciones de BlackBerry Dynamics" en el contenido de Administración.

Flujo de datos: activación de un dispositivo con Android Enterprise Trabajo y personal: privacidad de usuario mediante una cuenta de Google Play gestionada



Este flujo de datos se aplica cuando permite que BlackBerry UEM gestione cuentas de Google Play. Para obtener más información, consulte el contenido de Administración.

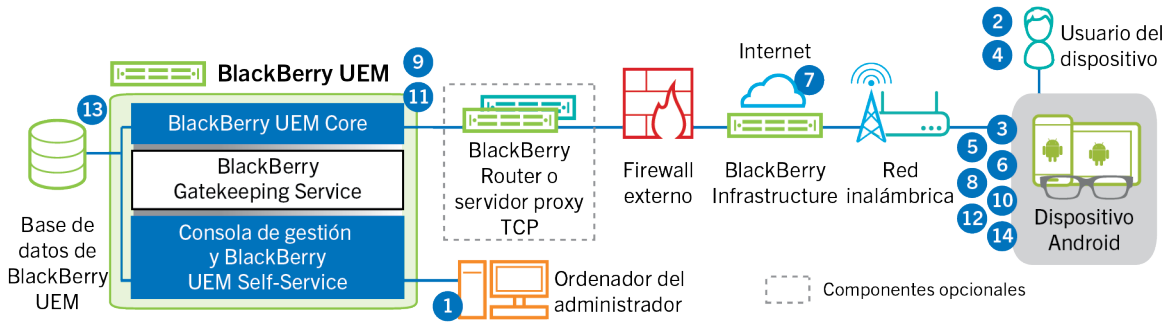
1. Lleve a cabo las acciones siguientes:
   a. Agregue un usuario a BlackBerry UEM como una cuenta de usuario local o mediante la información de la cuenta recuperada desde el directorio de la empresa.
   b. Asegúrese de haber asignado al usuario el tipo de activación "Trabajo y personal: privacidad de usuario".
   c. Utilice una de las siguientes opciones para proporcionar al usuario los detalles de activación:
      - Genere automáticamente una contraseña de activación del dispositivo y, de manera opcional, un QR Code y envíe un mensaje de correo electrónico con las instrucciones de activación al usuario
      - Establezca una contraseña de activación del dispositivo y comunique el nombre de usuario y la contraseña al usuario directamente o por correo electrónico

- Anule la configuración de la contraseña de activación y comunique la dirección de BlackBerry UEM Self-Service al usuario para que pueda establecer su propia contraseña de activación y ver un QR Code.

2. El usuario se descarga BlackBerry UEM Client de Google Play y lo instala en el dispositivo. Una vez instalado, el usuario abre BlackBerry UEM Client e introduce su dirección de correo electrónico y la contraseña de activación o escanea el QR Code.
3. BlackBerry UEM Client en el dispositivo lleva a cabo las siguientes acciones:
   a. Establece una conexión con BlackBerry Infrastructure
   b. Envía una solicitud para obtener la información de activación a BlackBerry Infrastructure
4. BlackBerry Infrastructure realiza las siguientes acciones:
   a. Comprueba que el usuario sea un usuario válido y registrado
   b. Recupera la dirección de BlackBerry UEM para el usuario
   c. Envía la dirección a BlackBerry UEM Client
5. BlackBerry UEM Client establece una conexión con BlackBerry UEM con el comando CONEXIÓN HTTP por el puerto 443 y envía una solicitud de activación a BlackBerry UEM. La solicitud de activación incluye el nombre de usuario, la contraseña, el sistema operativo del dispositivo y el identificador único del dispositivo.
6. BlackBerry UEM realiza las siguientes acciones:
   a. Determina el tipo de activación asignada a la cuenta de usuario
   b. Se conecta a Google y crea un usuario de Google Play gestionado
   c. Crea una instancia del dispositivo
   d. Asocia la instancia del dispositivo con la cuenta de usuario especificada
   e. Agrega el ID de la sesión de inscripción a una sesión HTTP
   f. Envía la información de la cuenta gestionada Google Play del usuario y un mensaje de autenticación satisfactoria al dispositivo
7. Si el dispositivo no está cifrado, se le pide al usuario que lo cifre.
8. BlackBerry UEM Client realiza las siguientes acciones:
   a. Se conecta a Google para verificar el usuario
   b. Crea el perfil de trabajo en el dispositivo
   c. Crea una CSR con la información recibida de BlackBerry UEM y envía una solicitud de certificado de cliente a BlackBerry UEM a través de HTTPS.
9. BlackBerry UEM realiza las siguientes acciones:
   a. Valida la solicitud del certificado de cliente con el ID de la sesión de inscripción en la sesión HTTP
   b. Firma la solicitud del certificado de cliente con el certificado raíz
   c. Envía el certificado de cliente firmado y el certificado raíz de nuevo a BlackBerry UEM Client

   Se establece una sesión TLS autenticada mutuamente entre BlackBerry UEM Client y BlackBerry UEM.
10. BlackBerry UEM Client solicita toda la información de configuración y envía la información del dispositivo y del software a BlackBerry UEM.
11. BlackBerry UEM almacena la información del dispositivo y envía la información de configuración al dispositivo.
12. El dispositivo envía una confirmación a BlackBerry UEM de que la ha recibido y aplica la información de configuración. El proceso de activación se ha completado.

Flujo de datos: activación de un dispositivo Android Enterprise Trabajo y personal: control total mediante una cuenta de Google Play gestionada



Este flujo de datos se aplica cuando permite que BlackBerry UEM gestione cuentas de Google Play. Para obtener más información, consulte el contenido de Administración.

1. Lleve a cabo las acciones siguientes:
   a. Agregue un usuario a BlackBerry UEM como una cuenta de usuario local o mediante la información de la cuenta recuperada desde el directorio de la empresa
   b. Asegúrese de que se ha asignado al usuario el tipo de activación "Trabajo y personal: control total"
   c. Configure los códigos QR de activación para que incluyan la contraseña de activación y la ubicación desde la que debe descargarse BlackBerry UEM Client.
2. El usuario restablece la configuración predeterminada de fábrica del dispositivo.
3. El dispositivo se reinicia y muestra una pantalla de bienvenida o de inicio.
4. El usuario realiza las siguientes acciones:
   a. Abre el correo electrónico de activación que ha recibido en su ordenador o en otro dispositivo
   b. Toca la pantalla del dispositivo siete veces para abrir un lector de códigos QR
   c. Conecta el dispositivo a una red Wi-Fi
   d. Escanea el código QR del correo electrónico de activación
5. El dispositivo realiza las siguientes acciones:
   a. Solicita al usuario que cifre el dispositivo y lo reinicie
   b. Descarga UEM Client de la ubicación de descarga especificada por el código QR y lo instala
6. UEM Client realiza las siguientes acciones:
   a. Establece una conexión con BlackBerry Infrastructure
   b. Envía una solicitud para obtener la información de activación a BlackBerry Infrastructure
7. BlackBerry Infrastructure realiza las siguientes acciones:
   a. Comprueba que el usuario sea un usuario válido y registrado
   b. Recupera la dirección del servidor de BlackBerry UEM para el usuario
   c. Envía la dirección del servidor a UEM Client
8. UEM Client establece una conexión con BlackBerry UEM con el comando CONEXIÓN HTTP por el puerto 443 y envía una solicitud de activación a BlackBerry UEM. La solicitud de activación incluye el nombre de usuario, la contraseña, el sistema operativo del dispositivo y el identificador único del dispositivo.
9. BlackBerry UEM realiza las siguientes acciones:
   a. Determina el tipo de activación asignada a la cuenta de usuario

b. Se conecta a Google y crea un usuario Google Play gestionado
c. Crea una instancia del dispositivo
d. Asocia la instancia del dispositivo con la cuenta de usuario especificada
e. Agrega el ID de la sesión de inscripción a una sesión HTTP
f. Envía la información de la cuenta gestionada Google Play del usuario y un mensaje de autenticación satisfactoria al dispositivo

10. UEM Client realiza las siguientes acciones:

a. Se conecta a Google para verificar el usuario
b. Crea el perfil de trabajo en el dispositivo
c. Crea una CSR con la información recibida de BlackBerry UEM y envía una solicitud de certificado de cliente a BlackBerry UEM a través de HTTPS

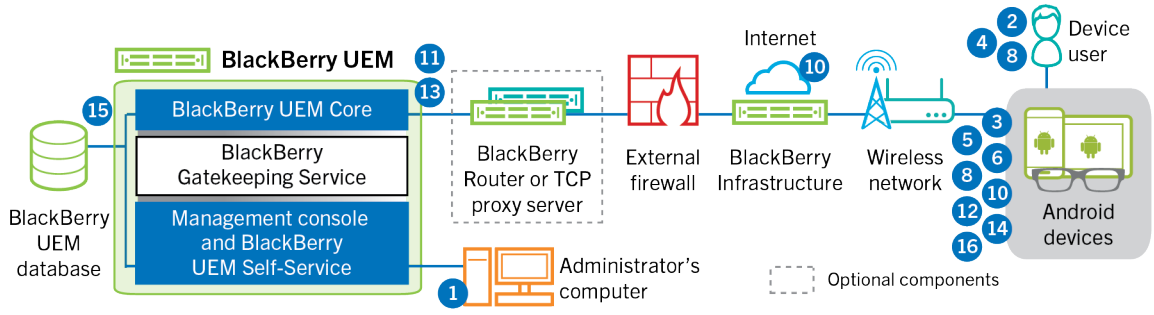
11. BlackBerry UEM realiza las siguientes acciones:

a. Valida la solicitud del certificado de cliente con el ID de la sesión de inscripción en la sesión HTTP
b. Firma la solicitud del certificado de cliente con el certificado raíz
c. Envía el certificado de cliente firmado y el certificado raíz de nuevo a UEM Client

Se establece una sesión TLS autenticada mutuamente entre UEM Client y BlackBerry UEM.

12. UEM Client solicita toda la información de configuración y envía la información del dispositivo y del software a BlackBerry UEM.
13. BlackBerry UEM almacena la información del dispositivo y envía la información de configuración al dispositivo.
14. El dispositivo envía una confirmación a BlackBerry UEM de que la ha recibido y aplica la información de configuración. El proceso de activación se ha completado.

Flujo de datos: activación de un dispositivo Android Enterprise Solo espacio de trabajo mediante una cuenta de Google Play gestionada



Este flujo de datos se aplica cuando permite que BlackBerry UEM gestione cuentas de Google Play. Para obtener más información, consulte el contenido de Administración.

1. Lleve a cabo las acciones siguientes:

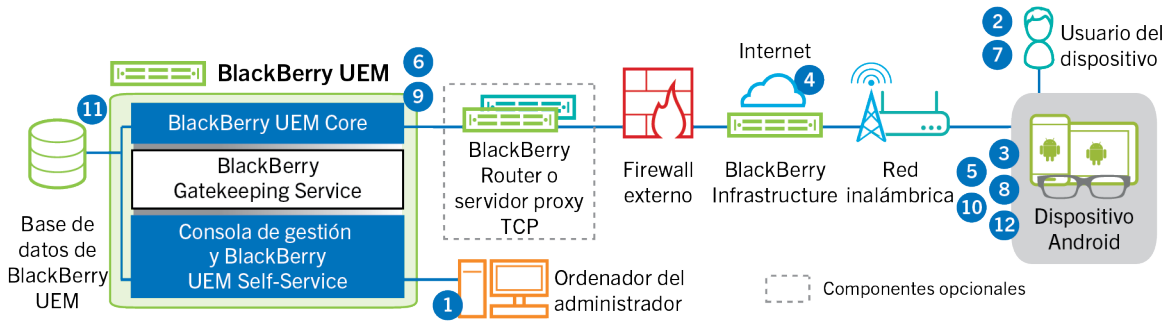
a. Agregue un usuario a BlackBerry UEM como una cuenta de usuario local o mediante la información de la cuenta recuperada desde el directorio de la empresa.
b. Asegúrese de que se ha asignado al usuario el tipo de activación "Solo espacio de trabajo"
c. Establezca la contraseña de activación del usuario.

2. El usuario restablece la configuración predeterminada de fábrica del dispositivo.
3. El dispositivo se reinicia e indica al usuario que seleccione una red Wi-Fi y agregue una cuenta.
4. El usuario introduce `afw#blackberry` en lugar del nombre de usuario de Google.

5. El dispositivo realiza las siguientes acciones:
   a. Si el dispositivo no está cifrado, solicita al usuario que cifre el dispositivo y se reinicia
   b. Descarga BlackBerry UEM Client desde Google Play y lo instala
6. BlackBerry UEM Client en el dispositivo solicita al usuario que introduzca su dirección de correo y la contraseña de activación.
7. El usuario escribe la dirección de correo y la contraseña de activación o escanea el QR Code.
8. BlackBerry UEM Client realiza las siguientes acciones:
   a. Establece una conexión con BlackBerry Infrastructure
   b. Envía una solicitud para obtener la información de activación a BlackBerry Infrastructure
9. BlackBerry Infrastructure realiza las siguientes acciones:
   a. Comprueba que el usuario sea un usuario válido y registrado
   b. Recupera la dirección del servidor BlackBerry UEM para el usuario
   c. Envía la dirección del servidor a BlackBerry UEM Client
10. BlackBerry UEM Client establece una conexión con BlackBerry UEM con el comando CONEXIÓN HTTP por el puerto 443 y envía una solicitud de activación a BlackBerry UEM. La solicitud de activación incluye el nombre de usuario, la contraseña, el sistema operativo del dispositivo y el identificador único del dispositivo.
11. BlackBerry UEM realiza las siguientes acciones:
   a. Determina el tipo de activación asignada a la cuenta de usuario
   b. Se conecta a Google y crea un usuario de Google Play gestionado
   c. Crea una instancia del dispositivo
   d. Asocia la instancia del dispositivo con la cuenta de usuario especificada
   e. Agrega el ID de la sesión de inscripción a una sesión HTTP
   f. Envía la información de la cuenta gestionada Google Play del usuario y un mensaje de autenticación satisfactoria al dispositivo
12. BlackBerry UEM Client realiza las siguientes acciones:
   a. Se conecta a Google para verificar el usuario
   b. Crea una CSR con la información recibida de BlackBerry UEM y envía una solicitud de certificado de cliente a BlackBerry UEM a través de HTTPS
13. BlackBerry UEM realiza las siguientes acciones:
   a. Valida la solicitud del certificado de cliente con el ID de la sesión de inscripción en la sesión HTTP
   b. Firma la solicitud del certificado de cliente con el certificado raíz
   c. Envía el certificado de cliente firmado y el certificado raíz de nuevo a BlackBerry UEM Client

   Se establece una sesión TLS autenticada mutuamente entre BlackBerry UEM Client y BlackBerry UEM.
14. BlackBerry UEM Client solicita toda la información de configuración y envía la información del dispositivo y del software a BlackBerry UEM.
15. BlackBerry UEM almacena la información del dispositivo y envía la información de configuración al dispositivo.
16. El dispositivo envía una confirmación a BlackBerry UEM de que la ha recibido y aplica la información de configuración. El proceso de activación se ha completado.

Flujo de datos: activación de un dispositivo Android Enterprise Trabajo y personal: privacidad de usuario en un dominio de Google



Este flujo de datos se aplica cuando BlackBerry UEM está conectado a un dominio de Google Cloud o G Suite. Para obtener más información, consulte el contenido de Administración.

1. Lleve a cabo las acciones siguientes:
   a. Compruebe que el usuario tiene una cuenta de Google que está asociada a la dirección de correo de trabajo del usuario. Opcionalmente, se puede configurar BlackBerry UEM para crear la cuenta de Google para el usuario durante el proceso de activación. Cuando BlackBerry UEM crea la cuenta de usuario en Google, el usuario recibe un correo electrónico desde el dominio de Google con la contraseña de la cuenta de Google.
   b. Agregue un usuario a BlackBerry UEM como una cuenta de usuario local o mediante la información de la cuenta recuperada desde el directorio de la empresa. Al especificar la dirección de correo electrónico, utilice la dirección de correo electrónico que se ha asociado a la cuenta de Google del usuario.
   c. Asegúrese de haber asignado al usuario el tipo de activación "Trabajo y personal: privacidad de usuario".
   d. Utilice una de las siguientes opciones para proporcionar al usuario los detalles de activación:
      - Genere automáticamente una contraseña de activación del dispositivo y, de manera opcional, un QR Code y envíe un mensaje de correo electrónico con las instrucciones de activación al usuario
      - Establezca una contraseña de activación del dispositivo y comunique el nombre de usuario y la contraseña al usuario directamente o por correo electrónico
      - Anule la configuración de la contraseña de activación y comunique la dirección de BlackBerry UEM Self-Service al usuario para que pueda establecer su propia contraseña de activación y ver un QR Code.
2. El usuario se descarga BlackBerry UEM Client de Google Play y lo instala en el dispositivo. Una vez instalado, el usuario abre BlackBerry UEM Client e introduce su dirección de correo electrónico y la contraseña de activación o escanea el QR Code.
3. BlackBerry UEM Client en el dispositivo lleva a cabo las siguientes acciones:
   a. Establece una conexión con BlackBerry Infrastructure
   b. Envía una solicitud para obtener la información de activación a BlackBerry Infrastructure
4. BlackBerry Infrastructure realiza las siguientes acciones:
   a. Comprueba que el usuario sea un usuario válido y registrado
   b. Recupera la dirección de BlackBerry UEM para el usuario
   c. Envía la dirección a BlackBerry UEM Client
5. BlackBerry UEM Client establece una conexión con BlackBerry UEM con el comando CONEXIÓN HTTP por el puerto 443 y envía una solicitud de activación a BlackBerry UEM. La solicitud de activación incluye el nombre de usuario, la contraseña, el sistema operativo del dispositivo y el identificador único del dispositivo.
6. BlackBerry UEM realiza las siguientes acciones:

a. Determina el tipo de activación asignada a la cuenta de usuario
b. Se conecta al dominio de Google administrado para verificar la información del usuario Si el usuario no existe, en función de su configuración, BlackBerry UEM puede crear el usuario en el dominio de Google
c. Crea una instancia del dispositivo
d. Asocia la instancia del dispositivo con la cuenta de usuario especificada
e. Agrega el ID de la sesión de inscripción a una sesión HTTP
f. Envía un mensaje de autenticación satisfactoria al dispositivo

7. Si el dispositivo no está cifrado, se le pide al usuario que lo cifre.
8. BlackBerry UEM Client realiza las siguientes acciones:

a. Crea el perfil de trabajo en el dispositivo
b. Solicita al usuario la información de la cuenta de Google del usuario
c. Se conecta al dominio de Google gestionado para autenticar al usuario
d. Crea el perfil de trabajo en el dispositivo
e. Crea una CSR con la información recibida de BlackBerry UEM y envía una solicitud de certificado de cliente a BlackBerry UEM a través de HTTPS.

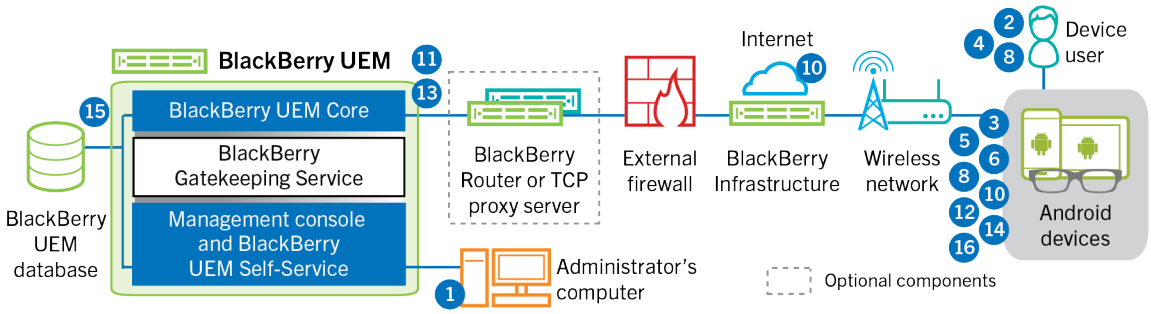
9. BlackBerry UEM realiza las siguientes acciones:

a. Valida la solicitud del certificado de cliente con el ID de la sesión de inscripción en la sesión HTTP
b. Firma la solicitud del certificado de cliente con el certificado raíz
c. Envía el certificado de cliente firmado y el certificado raíz de nuevo a BlackBerry UEM Client

Se establece una sesión TLS autenticada mutuamente entre BlackBerry UEM Client y BlackBerry UEM.

10. BlackBerry UEM Client solicita toda la información de configuración y envía la información del dispositivo y del software a BlackBerry UEM.
11. BlackBerry UEM almacena la información del dispositivo y envía la información de configuración solicitada al dispositivo.
12. El dispositivo envía una confirmación a BlackBerry UEM de que la ha recibido y aplica la información de configuración. El proceso de activación se ha completado.

Flujo de datos: activación de un dispositivo Android Enterprise Trabajo y personal: control total en un dominio de Google



Este flujo de datos se aplica cuando BlackBerry UEM está conectado a un dominio de Google Cloud o G Suite. Para obtener más información, consulte el contenido de Administración.

1. Lleve a cabo las acciones siguientes:

a. Compruebe que el usuario tiene una cuenta de Google que está asociada a la dirección de correo de trabajo del usuario. Opcionalmente, se puede configurar BlackBerry UEM para crear la cuenta de Google

para el usuario durante el proceso de activación. Cuando BlackBerry UEM crea la cuenta de usuario en Google, el usuario recibe un correo electrónico desde el dominio de Google con la contraseña de la cuenta de Google.

   b. Compruebe que la configuración "Aplicar política de EMM" esté activada para el dominio de Google. Este ajuste especifica que los dispositivos activados son administrados por un proveedor de EMM, como BlackBerry UEM.

   c. Agregue un usuario a BlackBerry UEM como una cuenta de usuario local o mediante la información de la cuenta recuperada desde el directorio de la empresa. Al especificar la dirección de correo electrónico, utilice la dirección de correo electrónico que se ha asociado a la cuenta de Google del usuario.

   d. Asegúrese de que se ha asignado al usuario el tipo de activación "Trabajo y personal: control total".

   e. Establezca la contraseña de activación del usuario.

2. El usuario restablece la configuración predeterminada de fábrica del dispositivo.
3. El dispositivo se reinicia e indica al usuario que seleccione una red Wi-Fi y agregue una cuenta.
4. El usuario tiene que introducir su dirección de correo electrónico y contraseña.
5. En el caso de los dispositivos con Google, se comunica con el dominio para verificar que el usuario es un usuario de trabajo y comprobar que la configuración "Aplicar política de EMM" esté activada. Después de realizar las validaciones pertinentes, el dispositivo realiza las siguientes acciones:

   a. Si el dispositivo no está cifrado, solicita al usuario que cifre el dispositivo y se reinicia

   b. Descarga BlackBerry UEM Client desde Google Play y lo instala

6. BlackBerry UEM Client en el dispositivo solicita al usuario que introduzca su dirección de correo y la contraseña de activación.
7. El usuario escribe la dirección de correo y la contraseña de activación o escanea el QR Code.
8. BlackBerry UEM Client en el dispositivo lleva a cabo las siguientes acciones:

   a. Establece una conexión con BlackBerry Infrastructure

   b. Envía una solicitud para obtener la información de activación a BlackBerry Infrastructure

9. BlackBerry Infrastructure realiza las siguientes acciones:

   a. Comprueba que el usuario sea un usuario válido y registrado

   b. Recupera la dirección del servidor BlackBerry UEM para el usuario

   c. Envía la dirección del servidor a BlackBerry UEM Client

10. BlackBerry UEM Client establece una conexión con BlackBerry UEM con el comando CONEXIÓN HTTP por el puerto 443 y envía una solicitud de activación a BlackBerry UEM. La solicitud de activación incluye el nombre de usuario, la contraseña, el sistema operativo del dispositivo y el identificador único del dispositivo.
11. BlackBerry UEM realiza las siguientes acciones:

   a. Determina el tipo de activación asignada a la cuenta de usuario

   b. Se conecta al dominio de Google para verificar la información del usuario Si el usuario no existe, en función de su configuración, BlackBerry UEM puede crear el usuario en el dominio de Google

   c. Crea una instancia del dispositivo

   d. Asocia la instancia del dispositivo con la cuenta de usuario especificada

   e. Agrega el ID de la sesión de inscripción a una sesión HTTP

   f. Envía un mensaje de autenticación satisfactoria al dispositivo

12. BlackBerry UEM Client realiza las siguientes acciones:

   a. Crea el perfil de trabajo en el dispositivo

   b. Solicita al usuario la información de la cuenta de Google del usuario

   c. Se conecta al dominio de Google para autenticar al usuario

   d. Crea una CSR con la información recibida de BlackBerry UEM y envía una solicitud de certificado de cliente a BlackBerry UEM a través de HTTPS

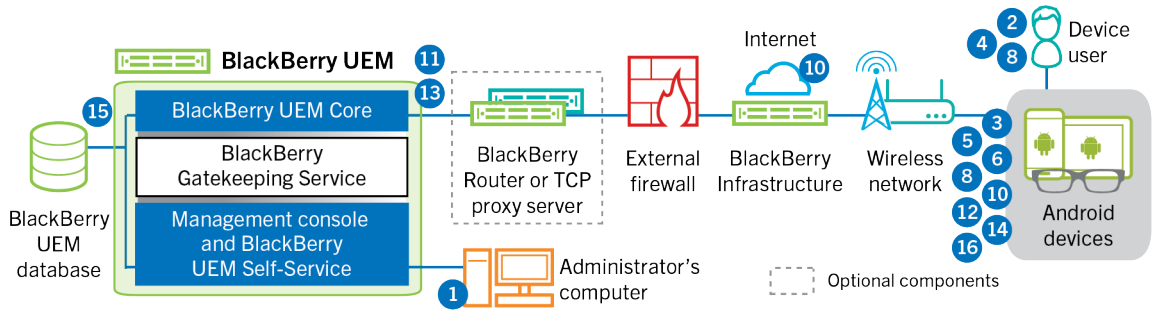
13. BlackBerry UEM realiza las siguientes acciones:

a. Valida la solicitud del certificado de cliente con el ID de la sesión de inscripción en la sesión HTTP
b. Firma la solicitud del certificado de cliente con el certificado raíz
c. Envía el certificado de cliente firmado y el certificado raíz de nuevo a BlackBerry UEM Client

Se establece una sesión TLS autenticada mutuamente entre BlackBerry UEM Client y BlackBerry UEM.

14. BlackBerry UEM Client solicita toda la información de configuración y envía la información del dispositivo y del software a BlackBerry UEM.
15. BlackBerry UEM almacena la información del dispositivo y envía la información de configuración solicitada al dispositivo.
16. El dispositivo envía una confirmación a BlackBerry UEM de que la ha recibido y aplica la información de configuración. El proceso de activación se ha completado.

Flujo de datos: activación de un dispositivo Android Enterprise Solo espacio de trabajo en un dominio de Google



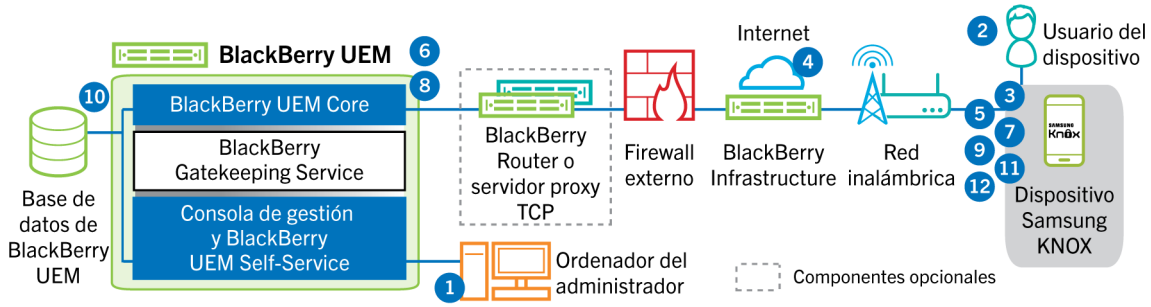
Este flujo de datos se aplica cuando BlackBerry UEM está conectado a un dominio de Google Cloud o G Suite. Para obtener más información, consulte el contenido de Administración.

1. Lleve a cabo las acciones siguientes:
   a. Compruebe que el usuario tiene una cuenta de Google que está asociada a la dirección de correo de trabajo del usuario. Opcionalmente, se puede configurar BlackBerry UEM para crear la cuenta de Google para el usuario durante el proceso de activación. Cuando BlackBerry UEM crea la cuenta de usuario en Google, el usuario recibe un correo electrónico desde el dominio de Google con la contraseña de la cuenta de Google.
   b. Compruebe que la configuración "Aplicar política de EMM" esté activada para el dominio de Google. Este ajuste especifica que los dispositivos activados son administrados por un proveedor de EMM, como BlackBerry UEM.
   c. Agregue un usuario a BlackBerry UEM como una cuenta de usuario local o mediante la información de la cuenta recuperada desde el directorio de la empresa. Al especificar la dirección de correo electrónico, utilice la dirección de correo electrónico que se ha asociado a la cuenta de Google del usuario.
   d. Asegúrese de que se ha asignado al usuario el tipo de activación "Solo espacio de trabajo".
   e. Establezca la contraseña de activación del usuario.
2. El usuario restablece la configuración predeterminada de fábrica del dispositivo.
3. El dispositivo se reinicia e indica al usuario que seleccione una red Wi-Fi y agregue una cuenta.
4. El usuario tiene que introducir su dirección de correo electrónico y contraseña.
5. En el caso de los dispositivos con Google, se comunica con el dominio para verificar que el usuario es un usuario de trabajo y comprobar que la configuración "Aplicar política de EMM" esté activada. Después de realizar las validaciones pertinentes, el dispositivo realiza las siguientes acciones:

   a. Si el dispositivo no está cifrado, solicita al usuario que cifre el dispositivo y se reinicia
   b. Descarga BlackBerry UEM Client desde Google Play y lo instala
6. BlackBerry UEM Client en el dispositivo solicita al usuario que introduzca su dirección de correo y la contraseña de activación.
7. El usuario escribe la dirección de correo y la contraseña de activación o escanea el QR Code.
8. BlackBerry UEM Client en el dispositivo lleva a cabo las siguientes acciones:
   a. Establece una conexión con BlackBerry Infrastructure
   b. Envía una solicitud para obtener la información de activación a BlackBerry Infrastructure
9. BlackBerry Infrastructure realiza las siguientes acciones:
   a. Comprueba que el usuario sea un usuario válido y registrado
   b. Recupera la dirección del servidor BlackBerry UEM para el usuario
   c. Envía la dirección del servidor a BlackBerry UEM Client
10. BlackBerry UEM Client establece una conexión con BlackBerry UEM con el comando CONEXIÓN HTTP por el puerto 443 y envía una solicitud de activación a BlackBerry UEM. La solicitud de activación incluye el nombre de usuario, la contraseña, el sistema operativo del dispositivo y el identificador único del dispositivo.
11. BlackBerry UEM realiza las siguientes acciones:
   a. Determina el tipo de activación asignada a la cuenta de usuario
   b. Se conecta al dominio de Google para verificar la información del usuario Si el usuario no existe, en función de su configuración, BlackBerry UEM puede crear el usuario en el dominio de Google
   c. Crea una instancia del dispositivo
   d. Asocia la instancia del dispositivo con la cuenta de usuario especificada
   e. Agrega el ID de la sesión de inscripción a una sesión HTTP
   f. Envía un mensaje de autenticación satisfactoria al dispositivo
12. BlackBerry UEM Client realiza las siguientes acciones:
   a. Solicita al usuario la información de la cuenta de Google del usuario
   b. Se conecta al dominio de Google para autenticar al usuario
   c. Crea una CSR con la información recibida de BlackBerry UEM y envía una solicitud de certificado de cliente a BlackBerry UEM a través de HTTPS
13. BlackBerry UEM realiza las siguientes acciones:
   a. Valida la solicitud del certificado de cliente con el ID de la sesión de inscripción en la sesión HTTP
   b. Firma la solicitud del certificado de cliente con el certificado raíz
   c. Envía el certificado de cliente firmado y el certificado raíz de nuevo a BlackBerry UEM Client

   Se establece una sesión TLS autenticada mutuamente entre BlackBerry UEM Client y BlackBerry UEM.
14. BlackBerry UEM Client solicita toda la información de configuración y envía la información del dispositivo y del software a BlackBerry UEM.
15. BlackBerry UEM almacena la información del dispositivo y envía la información de configuración solicitada al dispositivo.
16. El dispositivo envía una confirmación a BlackBerry UEM de que la ha recibido y aplica la información de configuración. El proceso de activación se ha completado.

Flujo de datos: activación de un dispositivo para que utilice Knox Workspace



1. Lleve a cabo las acciones siguientes:
   a. Agregue un usuario a BlackBerry UEM como una cuenta de usuario local o mediante la información de la cuenta recuperada desde el directorio de la empresa.
   b. Asegúrese de haber asignado al usuario el tipo de activación "Trabajo y personal: control total (Samsung Knox)", "Trabajo y personal: privacidad de usuario (Samsung Knox)" o "Solo espacio de trabajo - (Samsung Knox)"
   c. Utilice una de las siguientes opciones para proporcionar al usuario los detalles de activación:
      - Genere automáticamente una contraseña de activación del dispositivo y, de manera opcional, un QR Code y envíe un mensaje de correo electrónico con las instrucciones de activación al usuario
      - Establezca una contraseña de activación del dispositivo y comunique el nombre de usuario y la contraseña al usuario directamente o por correo electrónico
      - Anule la configuración de la contraseña de activación y comunique la dirección de BlackBerry UEM Self-Service al usuario para que pueda establecer su propia contraseña de activación y ver un QR Code.
2. El usuario descarga e instala BlackBerry UEM Client en el dispositivo. Una vez instalado, el usuario abre BlackBerry UEM Client e introduce la dirección de correo electrónico y la contraseña de activación o escanea el QR Code.
3. BlackBerry UEM Client realiza las siguientes acciones:
   a. Establece una conexión con BlackBerry Infrastructure
   b. Envía una solicitud para obtener la información de activación a BlackBerry Infrastructure
4. BlackBerry Infrastructure realiza las siguientes acciones:
   a. Comprueba que el usuario sea un usuario válido y registrado
   b. Recupera la dirección de BlackBerry UEM para el usuario
   c. Envía la dirección a BlackBerry UEM Client
5. BlackBerry UEM Client establece una conexión con BlackBerry UEM con el comando CONEXIÓN HTTP por el puerto 443 y envía una solicitud de activación a BlackBerry UEM. La solicitud de activación incluye el nombre de usuario, la contraseña, el sistema operativo del dispositivo y el identificador único del dispositivo.
6. BlackBerry UEM lleva a cabo las siguientes acciones:
   a. Inspecciona la validez de las credenciales
   b. Crea una instancia del dispositivo
   c. Asocia la instancia del dispositivo a la cuenta de usuario especificada en la base de datos de BlackBerry UEM
   d. Agrega el ID de la sesión de inscripción a una sesión HTTP
   e. Envía un mensaje de autenticación satisfactoria al dispositivo

7. BlackBerry UEM Client crea una CSR con la información recibida de BlackBerry UEM y envía una solicitud de certificado de cliente a BlackBerry UEM a través de HTTPS.
8. BlackBerry UEM realiza las siguientes acciones:

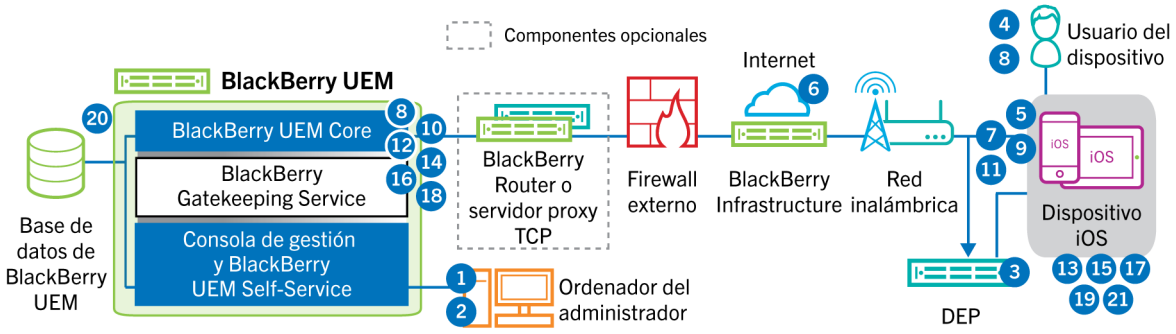
   a. Valida la solicitud del certificado de cliente con el ID de la sesión de inscripción en la sesión HTTP
   b. Firma la solicitud del certificado de cliente con el certificado raíz
   c. Envía el certificado de cliente firmado y el certificado raíz de nuevo a BlackBerry UEM Client

   Se establece una sesión TLS autenticada mutuamente entre BlackBerry UEM Client y BlackBerry UEM.
9. BlackBerry UEM Client solicita toda la información de configuración y envía la información del dispositivo y del software a BlackBerry UEM.
10. BlackBerry UEM almacena la información del dispositivo y envía la información de configuración al dispositivo.
11. BlackBerry UEM Client determina si el dispositivo utiliza Knox Workspace y si ejecuta una versión compatible. Si el dispositivo utiliza Knox Workspace MDM, el dispositivo se conecta a la infraestructura de Samsung y activa la licencia de administración de Knox. Tras la activación, BlackBerry UEM Client aplica el Knox MDM y las reglas de la política de TI de Knox Workspace.
12. El dispositivo envía una confirmación a BlackBerry UEM de que la ha recibido y aplica la información de configuración. El proceso de activación se ha completado.

Una vez haya finalizado la activación, se le pide al usuario que cree una contraseña del espacio de trabajo para Knox Workspace. Los datos de Knox Workspace estarán protegidos mediante cifrado y un método de autenticación como una contraseña, PIN, patrón o huella digital.

Nota: Si el dispositivo está activado con el tipo de activación "Solo espacio de trabajo - (Samsung Knox)", el espacio personal se eliminará cuando se configure Knox Workspace.

Flujo de datos: activación de un dispositivo iOS



1. Si tiene previsto utilizar el programa de inscripción de dispositivos de Apple, deberá realizar las siguientes acciones:

   a. Asegurarse de que BlackBerry UEM está configurado para sincronizar con DEP.
   b. Registrar el dispositivo en DEP y asignarlo a un servidor MDM
   c. Asignar una configuración de inscripción al dispositivo
2. Lleve a cabo las acciones siguientes:

   a. Agregue un usuario a BlackBerry UEM como una cuenta de usuario local o mediante la información de la cuenta recuperada desde el directorio de la empresa.
   b. Asigne un perfil de activación al usuario
   c. Utilice una de las siguientes opciones para proporcionar al usuario los detalles de activación:

      - Genere automáticamente una contraseña de activación del dispositivo y, de manera opcional, un QR Code y envíe un mensaje de correo electrónico con las instrucciones de activación al usuario

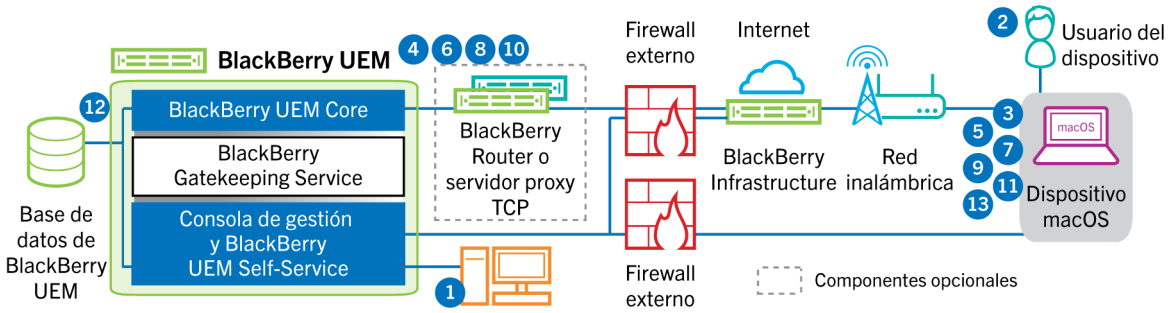
- Establezca una contraseña de activación del dispositivo y comunique el nombre de usuario y la contraseña al usuario directamente o por correo electrónico
- Anule la configuración de la contraseña de activación y comunique la dirección de BlackBerry UEM Self-Service al usuario para que pueda establecer su propia contraseña de activación y ver un QR Code.

3. Si el dispositivo se encuentra registrado en Apple DEP, este se comunicará con el servicio web de Apple DEP durante su configuración inicial. Si ha configurado el dispositivo para instalar la aplicación BlackBerry UEM Client, el dispositivo la descargará e instalará automáticamente.
4. Si el dispositivo no está registrado en Apple DEP o si no se ha configurado el dispositivo para instalar BlackBerry UEM Client, el usuario deberá descargar e instalar manualmente BlackBerry UEM Client en el dispositivo. Una vez instalado, el usuario abre BlackBerry UEM Client e introduce la dirección de correo electrónico y la contraseña de activación o escanea el QR Code.
5. BlackBerry UEM Client realiza las siguientes acciones:
   a. Establece una conexión con BlackBerry Infrastructure
   b. Envía una solicitud para obtener la información de activación a BlackBerry Infrastructure
6. BlackBerry Infrastructure realiza las siguientes acciones:
   a. Comprueba que el usuario sea un usuario válido y registrado
   b. Recupera la dirección de BlackBerry UEM para el usuario
   c. Envía la dirección a BlackBerry UEM Client
7. BlackBerry UEM Client establece una conexión con BlackBerry UEM con el comando CONEXIÓN HTTP por el puerto 443 y envía una solicitud de activación a BlackBerry UEM. La solicitud de activación incluye el nombre de usuario, la contraseña, el sistema operativo del dispositivo y el identificador único del dispositivo.
8. BlackBerry UEM lleva a cabo las siguientes acciones:
   a. Inspecciona la validez de las credenciales
   b. Crea una instancia del dispositivo
   c. Asocia la instancia del dispositivo a la cuenta de usuario especificada en la base de datos de BlackBerry UEM
   d. Agrega el ID de la sesión de inscripción a una sesión HTTP
   e. Envía un mensaje de autenticación satisfactoria al dispositivo
9. BlackBerry UEM Client crea una CSR con la información recibida de BlackBerry UEM y envía una solicitud de certificado de cliente a través de HTTPS.
10. BlackBerry UEM realiza las siguientes acciones:
    a. Valida la solicitud del certificado de cliente con el ID de la sesión de inscripción en la sesión HTTP
    b. Firma la solicitud del certificado de cliente con el certificado raíz
    c. Envía el certificado de cliente firmado y el certificado raíz de nuevo a BlackBerry UEM Client

    Se establece una sesión TLS autenticada mutuamente entre BlackBerry UEM Client y BlackBerry UEM.
11. BlackBerry UEM Client muestra un mensaje para informar al usuario de que el certificado debe instalarse para completar la activación. Cuando el usuario hace clic en Aceptar, se le redirige al vínculo para la activación del MDM Daemon nativo. BlackBerry UEM Client establece una conexión con BlackBerry UEM.
12. BlackBerry UEM proporciona el perfil de MDM al dispositivo. Este perfil contiene la URL de activación de MDM y contraseña de comprobación. El perfil de MDM está empaquetado como mensaje firmado PKCS#7 que incluye toda la cadena de certificados del firmante, lo que permite al dispositivo validar el perfil. Esto desencadena el proceso de inscripción.
13. El MDM Daemon nativo en el dispositivo envía el perfil del dispositivo, incluido el ID de cliente, el idioma y la versión del sistema operativo a BlackBerry UEM.
14. BlackBerry UEM valida que la solicitud esté firmada por una CA y responde al MDM Daemon nativo con una notificación de autenticación satisfactoria.
15. El MDM Daemon nativo envía una solicitud a BlackBerry UEM para pedir el certificado de CA, información sobre las capacidades de la CA y un certificado emitido por el dispositivo.

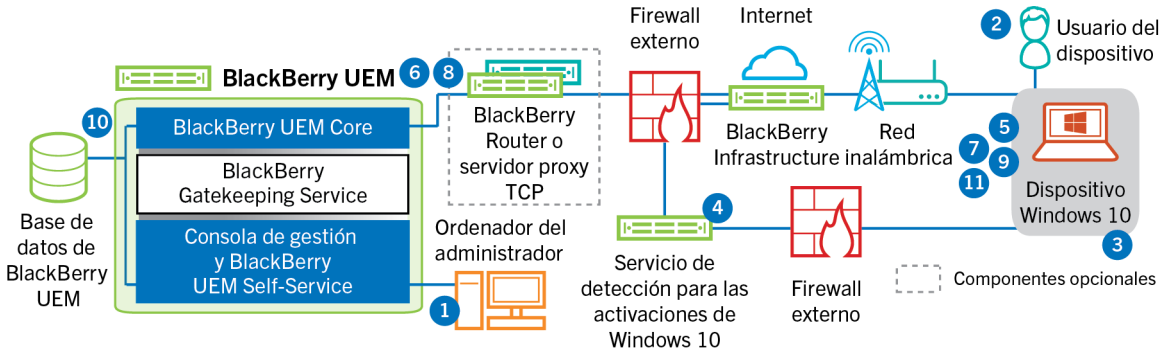
16. BlackBerry UEM envía el certificado de CA, la información de las capacidades de la CA y el certificado emitido por el dispositivo al MDM Daemon nativo.
17. El MDM Daemon nativo instala el perfil de MDM en el dispositivo. BlackBerry UEM Client notifica a BlackBerry UEM la correcta instalación del perfil MDM y del certificado, y sondea BlackBerry UEM periódicamente hasta confirmar que la activación de MDM ha finalizado.
18. BlackBerry UEM confirma que la activación de MDM ha finalizado.
19. BlackBerry UEM Client solicita toda la información de configuración y envía la información del dispositivo y del software a BlackBerry UEM.
20. BlackBerry UEM almacena la información del dispositivo y envía la información de configuración al dispositivo.
21. El dispositivo envía una confirmación a BlackBerry UEM de que la ha recibido y aplica las actualizaciones de configuración. El proceso de activación se ha completado.

Flujo de datos: activación de un dispositivo macOS



1. Asegúrese de que el usuario tenga una cuenta de usuario de BlackBerry UEM y la información de inicio de sesión de BlackBerry UEM Self-Service, incluidos:
   - Dirección web de BlackBerry UEM Self-Service
   - Nombre de usuario y contraseña
   - Nombre de dominio
2. El usuario inicia sesión en BlackBerry UEM Self-Service desde su dispositivo macOS y activa el dispositivo.
3. El dispositivo envía una solicitud de activación a BlackBerry UEM en el puerto 443.
4. BlackBerry UEM proporciona el perfil de MDM al dispositivo. Este perfil contiene la URL de activación de MDM y contraseña de comprobación. El perfil de MDM está empaquetado como mensaje firmado PKCS#7 que incluye toda la cadena de certificados del firmante, lo que permite al dispositivo validar el perfil. Esto desencadena el proceso de inscripción.
5. El MDM Daemon nativo en el dispositivo envía el perfil del dispositivo, incluido el ID de cliente, el idioma y la versión del sistema operativo a BlackBerry UEM.
6. BlackBerry UEM valida que la solicitud esté firmada por una CA y responde al MDM Daemon nativo con una notificación de autenticación satisfactoria.
7. El MDM Daemon nativo envía una solicitud a BlackBerry UEM para pedir el certificado de CA, información sobre las capacidades de la CA y un certificado emitido por el dispositivo.
8. BlackBerry UEM envía el certificado de CA, la información de las capacidades de la CA y el certificado emitido por el dispositivo al MDM Daemon nativo.
9. El MDM Daemon nativo instala el perfil de MDM en el dispositivo.
10. BlackBerry UEM confirma que la activación de MDM ha finalizado.
11. El dispositivo solicita toda la información de configuración.
12. BlackBerry UEM almacena la información del dispositivo y envía la información de configuración al dispositivo.
13. El dispositivo envía una confirmación a BlackBerry UEM de que la ha recibido y aplica la información de configuración. El proceso de activación se ha completado.

Flujo de datos: activación de un dispositivo Windows 10



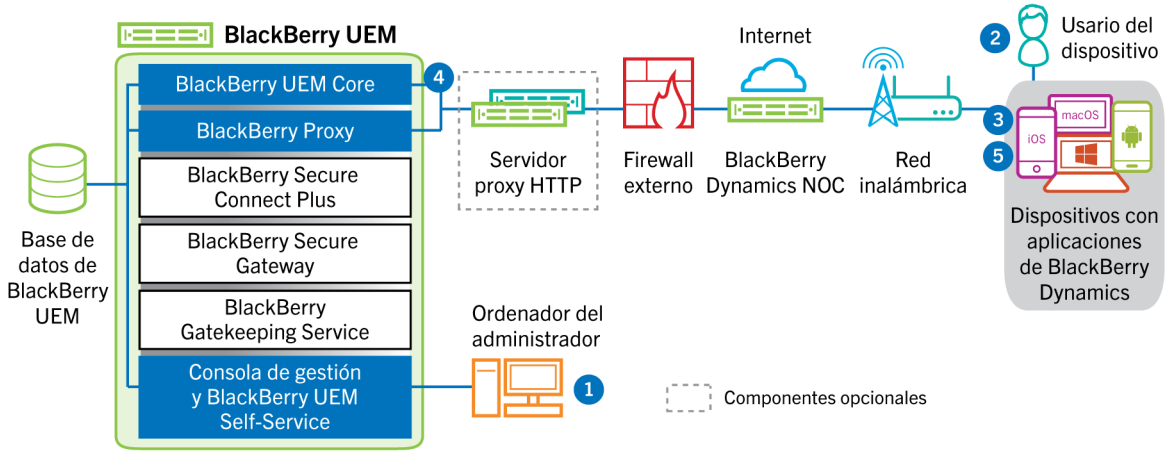
1. Lleve a cabo las acciones siguientes:
   a. Configurar el servicio de detección para simplificar las activaciones Windows 10
   b. Agregue un usuario a BlackBerry UEM como una cuenta de usuario local o mediante la información de la cuenta recuperada desde el directorio de la empresa.
   c. Utilice una de las siguientes opciones para proporcionar al usuario los detalles de activación:
      - Genere automáticamente una contraseña de activación del dispositivo y envíe un mensaje de correo con las instrucciones de activación al usuario.
      - Establezca una contraseña de activación del dispositivo y seleccione la opción para enviar la información de activación al usuario por correo.
      - Anule la configuración de la contraseña de activación y comunique la dirección de BlackBerry UEM Self-Service al usuario para que pueda establecer su propia contraseña de activación y consultar las direcciones del servidor.
   d. Proporcione al usuario un certificado CA generado por BlackBerry UEM para instalarlo en su dispositivo
2. El usuario realiza las siguientes acciones en el dispositivo:
   a. Comprueba que el dispositivo dispone de conectividad a Internet en el puerto 443
   b. Abre e instala el certificado
   c. Se dirige a Configuración > Cuentas > Espacio de trabajo y toca Conectar
   d. Cuando se le indica, introduce su dirección de correo y la contraseña de activación que recibió en el correo de activación
3. El dispositivo establece una conexión con el servicio de detección que configuró para simplificar las activaciones de Windows 10 de su empresa.
4. El servicio de detección comprueba que el ID de SRP para el servidor BlackBerry UEM es válido y redirige el dispositivo a BlackBerry UEM.
5. El dispositivo envía una solicitud de activación a BlackBerry UEM en el puerto 443. La solicitud de activación incluye el nombre de usuario, la contraseña, el sistema operativo del dispositivo y el identificador único del dispositivo.
6. BlackBerry UEM lleva a cabo las siguientes acciones:
   a. Inspecciona la validez de las credenciales
   b. Crea una instancia del dispositivo
   c. Asocia la instancia del dispositivo a la cuenta de usuario especificada en la base de datos de BlackBerry UEM
   d. Agrega el ID de la sesión de inscripción a una sesión HTTP
   e. Envía un mensaje de autenticación satisfactoria al dispositivo

7. El dispositivo crea una CSR y la envía a BlackBerry UEM a través de HTTPS. La CSR contiene el nombre de usuario y la contraseña de activación.
8. BlackBerry UEM valida el nombre de usuario y la contraseña, valida la CSR y devuelve el certificado de cliente y el certificado de CA al dispositivo.

   Todas las comunicaciones entre el dispositivo y BlackBerry UEM se someten ahora a una autenticación integral mutua mediante estos certificados.
9. El dispositivo solicita toda la información de configuración.
10. BlackBerry UEM almacena la información del dispositivo y envía la información de configuración al dispositivo.
11. El dispositivo envía una confirmación a BlackBerry UEM de que la ha recibido y aplica la información de configuración. El proceso de activación se ha completado.

Flujo de datos: activación de una aplicación de BlackBerry Dynamics por primera vez en un dispositivo

En este flujo de datos se describe cómo se desplazan los datos cuando se activa una aplicación de BlackBerry Dynamics en un dispositivo que no tiene otra aplicación de BlackBerry Dynamics ni BlackBerry UEM Client activados.



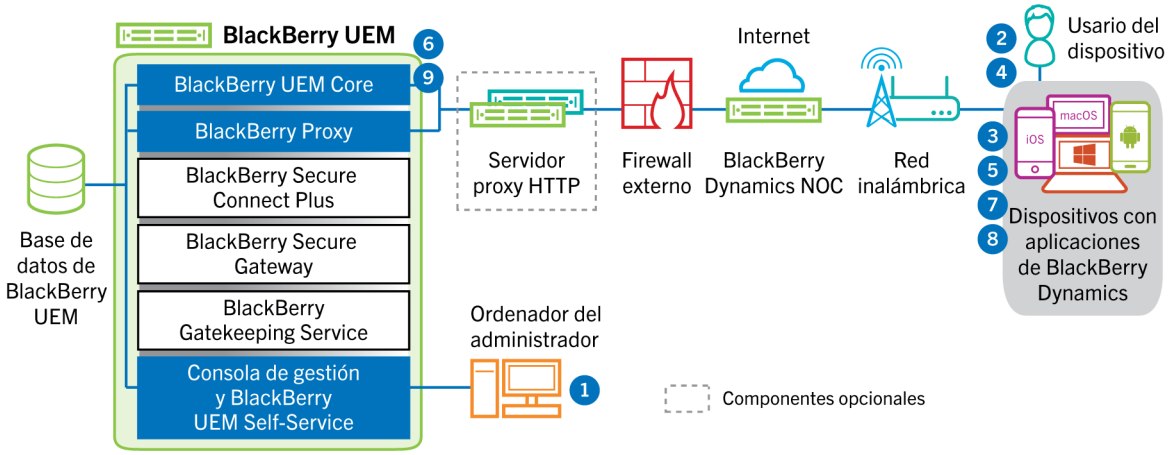
1. Un administrador realiza las siguientes acciones:
   a. Asigna una o más aplicaciones de BlackBerry Dynamics a un usuario.
   b. Emite las credenciales de activación (clave de acceso, contraseña de activación o código QR), o bien usa un proveedor de identidad de terceros, y las envía al usuario o indica al usuario que genere las credenciales desde BlackBerry UEM Self-Service.
2. El usuario realiza las siguientes acciones:
   a. Instala la aplicación en el dispositivo.
   b. Obtiene e introduce las credenciales de activación proporcionadas.
3. La aplicación de BlackBerry Dynamics realiza las acciones siguientes:
   a. Se conecta a BlackBerry Dynamics NOC y completa la activación.
   b. Obtiene la dirección de BlackBerry UEM mediante uno de los siguientes métodos:
      - Si el usuario introdujo manualmente las credenciales, la aplicación obtiene la dirección de BlackBerry Infrastructure.
      - Si el usuario ha escaneado un código QR, la aplicación recibe la dirección del código QR.
   c. Se conecta a BlackBerry UEM a través de BlackBerry Infrastructure y establece una sesión cifrada de manera integral con BlackBerry UEM mediante el protocolo EC-SPEKE.

      Esta sesión solo puede descifrarse mediante la instancia de BlackBerry UEM que emitió las credenciales de activación.
   d. Envía la solicitud de activación a través de la sesión segura.
4. BlackBerry UEM comprueba la solicitud de activación y envía una respuesta de activación cifrada a la aplicación. La respuesta de activación incluye los datos que necesita la aplicación para comunicarse con BlackBerry UEM, incluido un certificado de cliente, una clave de sesión principal, una lista de instancias de BlackBerry Proxy y autoridades de certificación de confianza.
5. La aplicación solicita al usuario que establezca una contraseña para la aplicación y que la registre como delegado de activación sencillo con BlackBerry Dynamics NOC para permitir que la siguiente aplicación de

BlackBerry Dynamics se active en el dispositivo sin que el usuario tenga que obtener manualmente nuevas credenciales.

Flujo de datos: activación de una aplicación de BlackBerry Dynamics cuando ya hay una activada en el dispositivo

En este flujo de datos se describe cómo se desplazan los datos cuando se activa una aplicación de BlackBerry Dynamics en un dispositivo que ya tiene BlackBerry UEM Client u otra aplicación de BlackBerry Dynamics activados y funcionando como delegado de activación sencillo.



1. Un administrador asigna una o más aplicaciones de BlackBerry Dynamics a un usuario.
2. El usuario instala la aplicación en el dispositivo.
3. La aplicación realiza las acciones siguientes:
   a. Consulta BlackBerry Dynamics NOC e identifica otra aplicación que esté activada en el dispositivo.
   b. Solicita las credenciales de activación de la aplicación activada anteriormente.
4. El usuario aprueba la solicitud de activación de la aplicación activada anteriormente en el dispositivo.
5. La aplicación activada anteriormente envía las credenciales a BlackBerry UEM.
6. BlackBerry UEM envía la solicitud de credenciales y la URL de BlackBerry UEM a la aplicación existente.
7. La aplicación activada anteriormente devuelve las credenciales y la URL a la nueva aplicación.
8. La nueva aplicación realiza las acciones siguientes:
   a. Se activa con BlackBerry Dynamics NOC.
   b. Se conecta a BlackBerry UEM a través de BlackBerry Infrastructure y establece una sesión cifrada de manera integral con BlackBerry UEM mediante el protocolo EC-SPEKE.

      Esta sesión solo puede descifrarse mediante la instancia de BlackBerry UEM que emitió las credenciales de activación.
   c. Envía la solicitud de activación a través de la sesión segura.
9. BlackBerry UEM comprueba la solicitud de activación y envía una respuesta de activación cifrada a la aplicación. La respuesta de activación incluye los datos que necesita la aplicación para comunicarse con BlackBerry UEM, incluido un certificado de cliente, una clave de sesión principal, una lista de instancias de BlackBerry Proxy y autoridades de certificación de confianza.

Envío y recepción de datos de trabajo

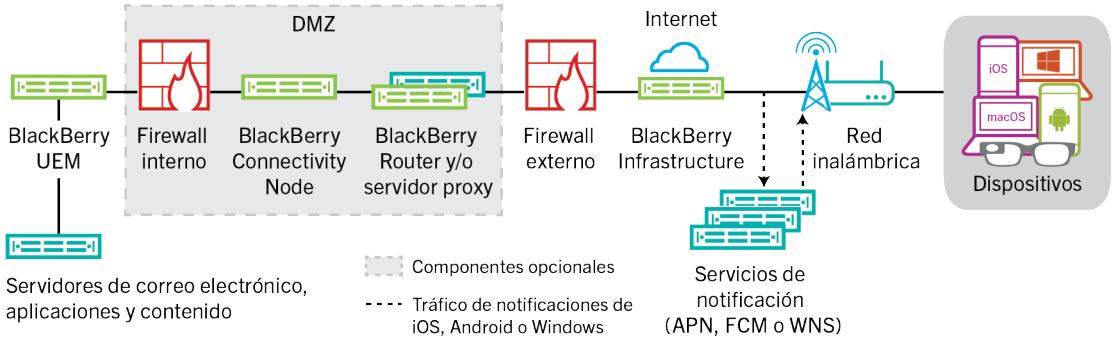
Cuando los dispositivos que están activos en BlackBerry UEM envían y reciben datos de trabajo, se conectan a los servidores de correo, de aplicaciones o de contenido de su empresa. Por ejemplo, cuando utilizan las aplicaciones de correo electrónico o de calendario del trabajo, los dispositivos establecen una conexión con el servidor de correo de la empresa. Cuando utilizan el navegador de trabajo para navegar por la intranet, los dispositivos establecen una conexión con el servidor web de empresa, y así sucesivamente.

En función del tipo de dispositivo, del tipo de activación, de los tipos de licencia y de los ajustes de configuración, un dispositivo puede establecer conexiones a los servidores de su empresa utilizando las siguientes rutas:

Ruta de datos	Descripción
Red Wi-Fi de trabajo	Puede utilizar BlackBerry UEM para configurar perfiles Wi-Fi para los dispositivos, de modo que estos puedan conectarse a los recursos de la empresa a través de su red Wi-Fi de trabajo.
VPN	Puede utilizar BlackBerry UEM para configurar perfiles VPN para los dispositivos, o bien los usuarios pueden configurar perfiles VPN en sus dispositivos para que estos puedan conectarse a los recursos de la empresa mediante una red VPN.
BlackBerry UEM y BlackBerry Infrastructure o BlackBerry Dynamics NOC	En función del dispositivo, de la activación y del tipo de licencia, y en la presencia de aplicaciones de BlackBerry Dynamics, es posible que los dispositivos puedan usar la conectividad de la empresa para comunicarse con los recursos de la empresa a través de BlackBerry UEM y BlackBerry Infrastructure. • Para dispositivos iOS, si dichos dispositivos cuentan con la licencia adecuada, puede activar BlackBerry Secure Gateway para permitir que los dispositivos se conecten al servidor de correo de trabajo a través de BlackBerry Infrastructure y BlackBerry UEM. Si utiliza BlackBerry Secure Gateway, no tendrá que exponer su servidor de correo fuera del firewall para permitir a los usuarios de dispositivos iOS conectarse a Microsoft Exchange cuando no están conectados a su red Wi-Fi de trabajo o de VPN. • Para dispositivos iOS, Android Enterprise, y Samsung Knox Workspace, si dichos dispositivos tienen una licencia adecuada, puede usar la conectividad de la empresa mediante la activación de BlackBerry Secure Connect Plus. Cuando los dispositivos utilizan BlackBerry Secure Connect Plus, los datos de trabajo se desplazan por un túnel IP seguro establecido entre las aplicaciones del dispositivo y la red de la empresa a través de BlackBerry Infrastructure. • Las aplicaciones de BlackBerry Dynamics instaladas en los dispositivos se comunican con BlackBerry Proxy. En función de su configuración, los datos pueden desplazarse a través de BlackBerry Dynamics NOC o BlackBerry Infrastructure, u omitirlos utilizando BlackBerry Dynamics Direct Connect. • Los dispositivos pueden utilizar la conectividad de la empresa para todos los datos de trabajo. La conectividad de la empresa cifra y autentica todos los datos de trabajo y los envía a través de BlackBerry UEM y BlackBerry Infrastructure. La conectividad de empresa limita el número de puertos que necesita abrir en el firewall externo de la empresa a un único puerto, el 3101.

Envío y recepción de datos de trabajo mediante BlackBerry Infrastructure

Los dispositivos se conectan a BlackBerry UEM a través de BlackBerry Infrastructure para obtener actualizaciones de configuración y para enviar y recibir datos de trabajo mediante la conectividad de la empresa o BlackBerry Secure Gateway. El diagrama siguiente muestra cómo se conectan los dispositivos a BlackBerry UEM y a los recursos de su empresa a través de BlackBerry Infrastructure.



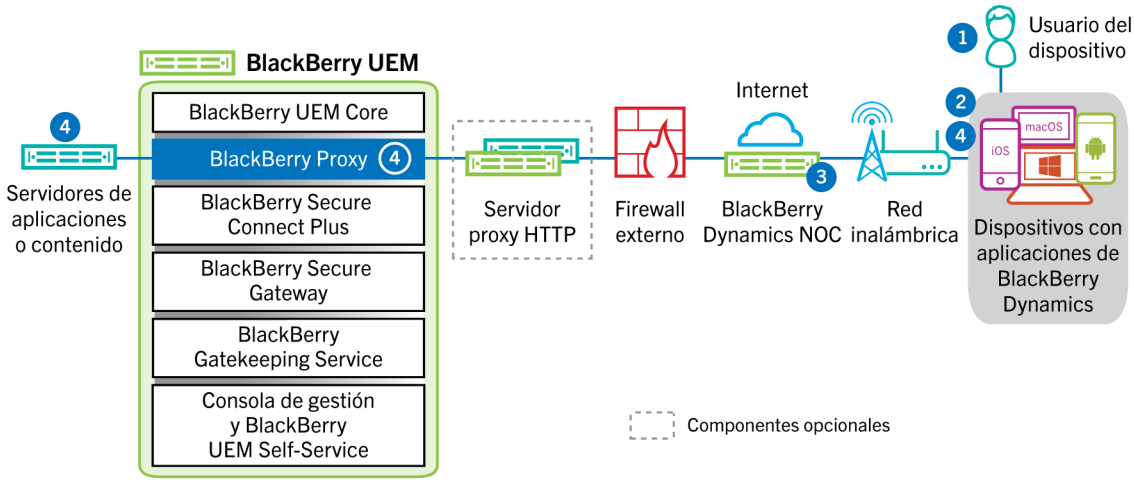
La tabla siguiente enumera las circunstancias en las que los dispositivos se conectan a BlackBerry UEM y a la red de su empresa a través de BlackBerry Infrastructure.

Tipo de dispositivo	Descripción
Todos los dispositivos	Todos los dispositivos utilizan esta ruta de comunicación para enviar y recibir datos de configuración como los comandos del dispositivo o las actualizaciones de políticas y perfiles, así como para enviar información sobre el dispositivo e informes de actividad. Para obtener más información, consulte Recepción de actualizaciones de configuración del dispositivo.
Dispositivos iOS	Puede activar BlackBerry Secure Gateway para permitir que los dispositivos iOS se conecten a su servidor de correo electrónico de trabajo a través de BlackBerry Infrastructure y BlackBerry UEM. Si utiliza BlackBerry Secure Gateway, no tendrá que exponer su servidor de correo fuera del firewall para permitir que los usuarios reciban correo de trabajo cuando no están conectados a la VPN de la empresa o a la red Wi-Fi de trabajo.

Tipo de dispositivo	Descripción
Dispositivos iOS, Android Enterprise y Samsung Knox Workspace.	Los dispositivos que tienen un perfil de conectividad de la empresa configurado para utilizar BlackBerry Secure Connect Plus pueden utilizar un túnel IP seguro a través de BlackBerry Infrastructure para transferir datos entre las aplicaciones y la red de la empresa. Para dispositivos iOS, BlackBerry Secure Connect Plus puede proporcionar un túnel seguro entre la red de su empresa y todas las aplicaciones o solo las aplicaciones especificadas. Para dispositivos con Android Enterprise, BlackBerry Secure Connect Plus, proporciona un túnel seguro entre todas las aplicaciones del espacio de trabajo y la red de su empresa. Para dispositivos Samsung Knox Workspace, BlackBerry Secure Connect Plus puede proporcionar un túnel seguro entre la red de su empresa y todas las aplicaciones de trabajo o solo las aplicaciones de trabajo especificadas.
Dispositivos iOS y Android con aplicaciones instaladas de BlackBerry Dynamics	La conectividad de la empresa para las aplicaciones de BlackBerry Dynamics no utiliza BlackBerry Infrastructure. En su lugar, los datos en tránsito entre las aplicaciones de BlackBerry Dynamics y BlackBerry Proxy pueden desplazarse a través de BlackBerry Dynamics NOC o pueden omitir el NOC mediante BlackBerry Dynamics Direct Connect.

Flujo de datos: envío y recepción de datos de trabajo desde una aplicación de BlackBerry Dynamics mediante BlackBerry Dynamics NOC

En este flujo de datos se describe cómo se desplazan los datos cuando una aplicación de BlackBerry Dynamics accede a un servidor de aplicaciones o de contenido en la empresa mediante BlackBerry Dynamics NOC BlackBerry UEM.



1. El usuario abre una aplicación de BlackBerry Dynamics para acceder a los datos de trabajo.
2. La aplicación de BlackBerry Dynamics establece una conexión con BlackBerry Dynamics NOC. La conexión está autenticada con la clave de enlace maestro que se creó cuando la aplicación se activó.
3. BlackBerry Dynamics NOC se comunica con BlackBerry Proxy a través de una conexión segura establecida previamente para establecer una conexión integral entre la aplicación de BlackBerry Dynamics y BlackBerry

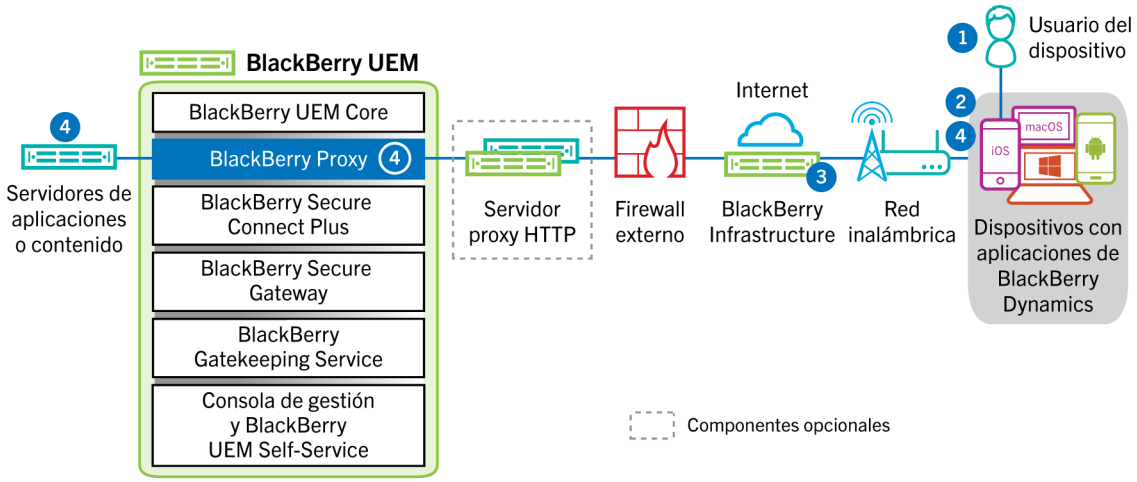
Proxy que transporta los datos de trabajo. Los datos de trabajo se cifran con una clave de sesión que BlackBerry Dynamics NOC no conoce.

4. Cuando se establece la conexión integral, los datos de trabajo se desplazan entre el dispositivo y los servidores de aplicaciones o de contenido detrás del firewall mediante BlackBerry Proxy.

Flujo de datos: envío y recepción de datos de trabajo desde una aplicación de BlackBerry Dynamics mediante BlackBerry Infrastructure

En función de la configuración del servidor, los datos de trabajo de las aplicaciones desarrolladas con BlackBerry Dynamics SDK 7.0 y versiones posteriores pueden desplazarse por BlackBerry Infrastructure en lugar de por BlackBerry Dynamics NOC. Si tiene una nueva instalación de BlackBerry UEM con la versión 12.12, BlackBerry UEM utiliza BlackBerry Infrastructure de forma predeterminada. Si actualiza desde una versión anterior de BlackBerry UEM, debe ponerse en contacto con el equipo de asistencia técnica de BlackBerry para activar esta función.

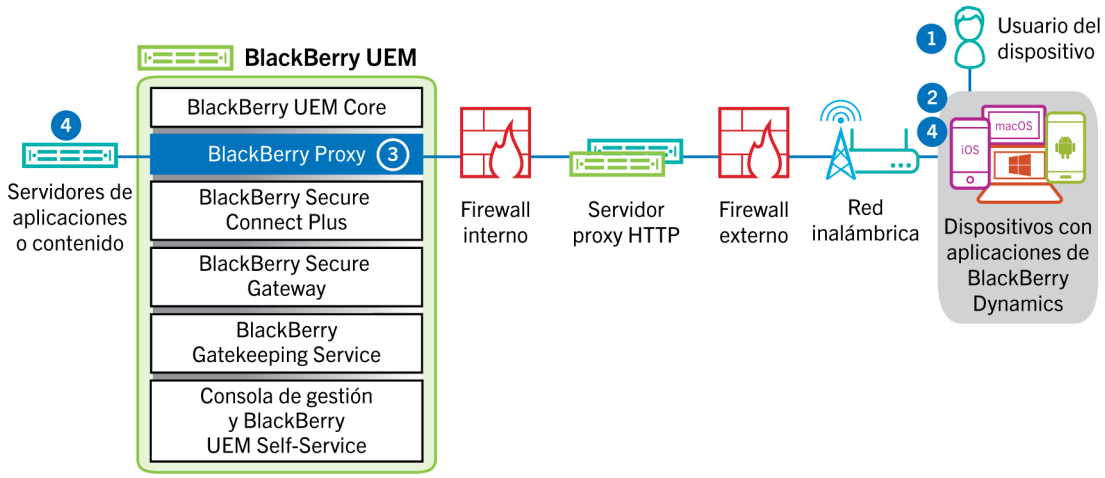
En este flujo de datos se describe cómo se desplazan los datos cuando una aplicación de BlackBerry Dynamics accede a un servidor de aplicaciones o de contenido en la empresa mediante BlackBerry Infrastructure BlackBerry UEM.



1. El usuario abre una aplicación de BlackBerry Dynamics para acceder a los datos de trabajo.
2. La aplicación de BlackBerry Dynamics establece una conexión con BlackBerry Infrastructure.
3. BlackBerry Infrastructure se comunica con BlackBerry Proxy a través de una conexión TLS establecida previamente.
4. La aplicación BlackBerry Dynamics establece una conexión TLS con BlackBerry Proxy y se intercambian datos de trabajo a través de una conexión segura integral.

Flujo de datos: envío y recepción de datos de trabajo desde una aplicación de BlackBerry Dynamics mediante BlackBerry Dynamics Direct Connect

En este flujo de datos se describe cómo se desplazan los datos cuando una aplicación de BlackBerry Dynamics accede a un servidor de aplicaciones o de contenido en la empresa mediante BlackBerry Dynamics Direct Connect y BlackBerry UEM. Para obtener más información acerca de Direct Connect, consulte Configuración de Direct Connect con BlackBerry UEM.

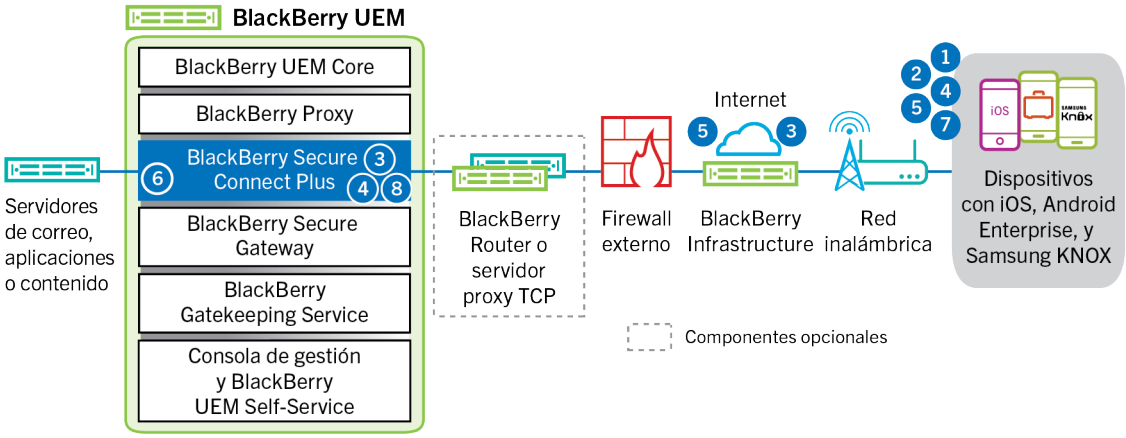


1. El usuario abre una aplicación de BlackBerry Dynamics para acceder a los datos de trabajo.
2. La aplicación de BlackBerry Dynamics establece una conexión TLS con BlackBerry Proxy.
3. BlackBerry Proxy se autentica con la aplicación de BlackBerry Dynamics. BlackBerry Proxy se autentica con la aplicación utilizando su certificado de servidor. BlackBerry Proxy valida la aplicación mediante una clave MAC con una clave de sesión que solo conoce BlackBerry Proxy y la aplicación.
4. Cuando se establece la conexión integral, los datos de trabajo se desplazan entre el dispositivo y los servidores de aplicaciones o de contenido detrás del firewall mediante BlackBerry Proxy.

Flujo de datos: acceso a un servidor de aplicaciones o contenido mediante BlackBerry Secure Connect Plus

Este flujo de datos describe cómo se desplazan los datos cuando una aplicación en un dispositivo que está configurado para utilizar BlackBerry Secure Connect Plus accede a un servidor de aplicaciones o de contenido de la empresa.

Este flujo de datos no se aplica a las aplicaciones de BlackBerry Dynamics del espacio de trabajo de dispositivos Android Enterprise o dispositivos Samsung Knox Workspace. Para obtener más información, consulte: Flujo de datos: envío y recepción de datos de trabajo desde una aplicación de BlackBerry Dynamics en un dispositivo Android utilizando BlackBerry Secure Connect Plus



1. El usuario abre una aplicación para acceder a los datos de trabajo desde un servidor de aplicaciones o de contenido detrás del firewall de la empresa.

- Para dispositivos Android Enterprise, todas las aplicaciones del espacio de trabajo utilizan BlackBerry Secure Connect Plus, con la excepción de aquellas que elija restringir.
- En los dispositivos Samsung Knox Workspace, puede especificar si todas las aplicaciones de espacio de trabajo o solo algunas utilizan BlackBerry Secure Connect Plus.
- En los dispositivos iOS, puede especificar si todas las aplicaciones o solo algunas utilizan BlackBerry Secure Connect Plus.

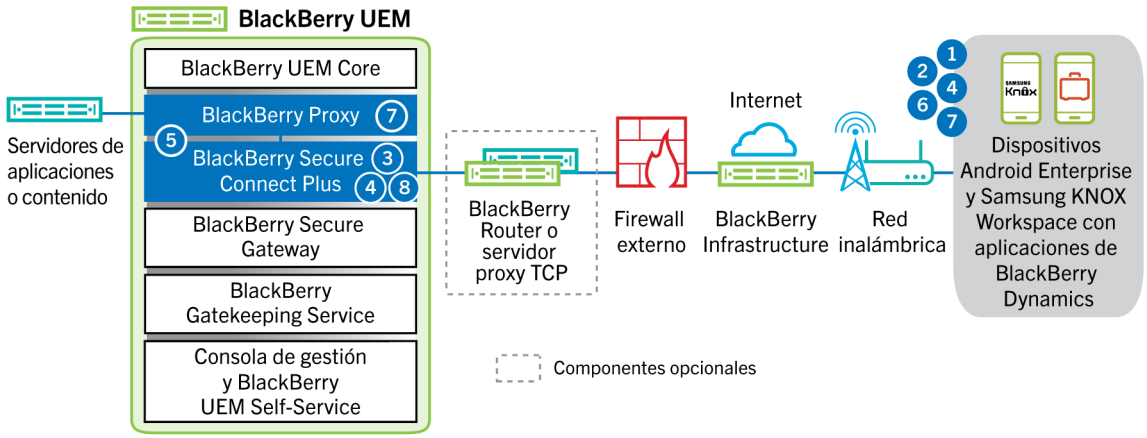
2. El dispositivo envía una solicitud a través de túnel TLS, a través del puerto 443, a BlackBerry Infrastructure para solicitar un túnel seguro a la red de trabajo. La señal se cifra de forma predeterminada con bibliotecas Certicom certificadas mediante FIPS-140. El túnel de señalización se somete a un cifrado integral.
3. BlackBerry Secure Connect Plus recibe la solicitud de BlackBerry Infrastructure a través del puerto 3101.
4. El dispositivo y BlackBerry Secure Connect Plus negocian los parámetros del túnel y establecen un túnel seguro para el dispositivo a través de BlackBerry Infrastructure. El túnel se autentica y se cifra de forma integral con DTLS.
5. La aplicación utiliza el túnel para conectarse con el servidor de aplicaciones o de contenido mediante protocolos estándar IPv4 (TCP y UDP).
6. BlackBerry Secure Connect Plus envía y recibe los datos de la IP desde la red de su empresa. BlackBerry Secure Connect Plus cifra y descifra el tráfico a través de bibliotecas Certicom certificadas mediante FIPS-140.
7. La aplicación recibe y muestra los datos en el dispositivo.
8. Mientras el túnel esté abierto, las aplicaciones compatibles lo utilizarán para acceder a los recursos de red. Cuando el túnel deja de ser el mejor método disponible para conectarse a la red de su empresa, BlackBerry Secure Connect Plus lo finaliza.

Flujo de datos: envío y recepción de datos de trabajo desde una aplicación de BlackBerry Dynamics en un dispositivo Android utilizando BlackBerry Secure Connect Plus

Este flujo de datos describe cómo viajan los datos cuando una aplicación de BlackBerry Dynamics en un dispositivo Android Enterprise o Samsung Knox Workspace utiliza BlackBerry Secure Connect Plus.

Si está utilizando BlackBerry Secure Connect Plus con aplicaciones de BlackBerry Dynamics en un dispositivo Android Enterprise, es recomendable restringir las aplicaciones de BlackBerry Dynamics para que no utilicen BlackBerry Secure Connect Plus con el fin de evitar la latencia de la red. No se pueden restringir aplicaciones específicas en dispositivos Samsung Knox Workspace.

Si está utilizando BlackBerry Secure Connect Plus con aplicaciones de BlackBerry Dynamics en un dispositivo Android Enterprise o un dispositivo Samsung Knox Workspace, es recomendable que configure BlackBerry UEM para que no envíe los datos de las aplicaciones de BlackBerry Dynamics a través de BlackBerry Dynamics NOC con el fin de reducir la latencia de la red.



1. El usuario abre una aplicación de BlackBerry Dynamics para acceder a los datos de trabajo.
2. El dispositivo envía una solicitud a través de túnel TLS, a través del puerto 443, a BlackBerry Infrastructure para solicitar un túnel seguro a la red de trabajo. La señal se cifra de forma predeterminada con bibliotecas Certicom certificadas mediante FIPS-140. El túnel de señalización se somete a un cifrado integral.
3. BlackBerry Secure Connect Plus recibe la solicitud de BlackBerry Infrastructure a través del puerto 3101.
4. El dispositivo y BlackBerry Secure Connect Plus negocian los parámetros del túnel y establecen un túnel seguro para el dispositivo a través de BlackBerry Infrastructure. El túnel se autentica y se cifra de forma integral con DTLS.
5. BlackBerry Secure Connect Plus establece una conexión con BlackBerry Proxy.
6. La aplicación de BlackBerry Dynamics establece una conexión con BlackBerry Proxy utilizando el túnel de BlackBerry Secure Connect Plus.
7. BlackBerry Proxy se autentica en la aplicación de BlackBerry Dynamics utilizando su certificado de servidor. BlackBerry Proxy valida la aplicación mediante una clave MAC con una clave de sesión que solo conoce BlackBerry Proxy y la aplicación.
8. Cuando se establece la conexión segura entre BlackBerry Proxy y la aplicación, los datos de trabajo se pueden desplazar entre el dispositivo y los servidores de aplicaciones o de contenido detrás del firewall utilizando el túnel de BlackBerry Secure Connect Plus a BlackBerry Proxy. BlackBerry Secure Connect Plus cifra y descifra el tráfico a través de bibliotecas Certicom certificadas mediante FIPS-140.

Flujo de datos: autenticación con el servidor de correo desde un dispositivo con iOS cuando se usa BlackBerry Secure Gateway

Este flujo de datos describe cómo los dispositivos con iOS 13 o una versión posterior se autentican con su servidor de correo a través de BlackBerry Secure Gateway mediante la autenticación moderna de Microsoft. Para obtener información sobre cómo configurar BlackBerry Secure Gateway para que haga uso de la autenticación moderna, consulte el contenido de administración.

Los siguientes pasos describen el flujo de datos estándar. Algunos detalles pueden variar según la configuración de su inquilino de Azure. Para obtener más información acerca de cómo el proveedor de identidad de Microsoft administra las solicitudes de autorización, consulte la documentación de Microsoft.

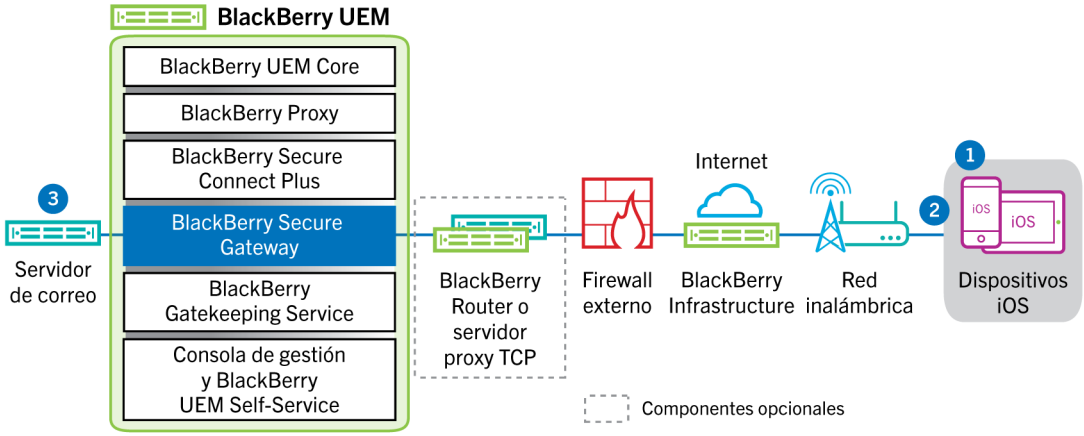
1. BlackBerry Secure Gateway recupera y almacena en caché los documentos de detección del servidor de autorización/proveedor de identidad especificados en los ajustes de configuración de BlackBerry Secure Gateway. BlackBerry Secure Gateway recupera tanto el documento de detección sin versión para dispositivos con iOS 13 y el documento de detección v2.0 para dispositivos con iOS 14.6 y versiones posteriores.
2. El dispositivo establece una conexión segura a través de BlackBerry Infrastructure con BlackBerry Secure Gateway.
3. BlackBerry Secure Gateway establece una conexión TLS con el servidor de autorización/proveedor de identidad especificado en los ajustes de configuración de BlackBerry Secure Gateway.
4. El dispositivo envía una solicitud de código de autorización a través de BlackBerry Secure Gateway con el servidor de autorización/proveedor de identidad.
5. El servidor de autorización/proveedor de identidad devuelve una respuesta de redireccionamiento HTTP 302 al dispositivo.
6. El dispositivo envía una solicitud de autorización a la URL especificada a través de la respuesta de redireccionamiento. La solicitud no se envía a través de BlackBerry Secure Gateway.
7. El servidor de autorización/proveedor de identidad envía una solicitud de autenticación de usuario al dispositivo. El tipo de solicitud (por ejemplo, una página de inicio de sesión o una solicitud de la aplicación de Microsoft Authenticator) y el flujo de mensajes para la autenticación del usuario dependen de la configuración de su inquilino de Azure.
8. El usuario proporciona las credenciales solicitadas al servidor de autorización/proveedor de identidad.

9. Cuando se completa la autenticación del usuario, el servidor de autorización/proveedor de identidad envía un código de autorización al dispositivo.
10. El dispositivo solicita el documento de detección del servidor de autorización/proveedor de identidad desde BlackBerry Secure Gateway.
11. BlackBerry Secure Gateway envía el documento de detección al dispositivo.
12. El dispositivo envía una solicitud de identificador de acceso a través de BlackBerry Secure Gateway al servidor de autorización/proveedor de identidad.
13. El servidor de autorización/proveedor de identidad envía el identificador de acceso al dispositivo.
14. Cuando envía o recibe un correo electrónico, el dispositivo presenta el identificador de acceso para establecer una conexión segura con el servidor de correo.

    Cuando el identificador de acceso caduca, el dispositivo envía una nueva solicitud de identificador a través de BlackBerry Secure Gateway al servidor de autorización/proveedor de identidad.

Flujo de datos: envío de correo desde un dispositivo iOS con BlackBerry Secure Gateway

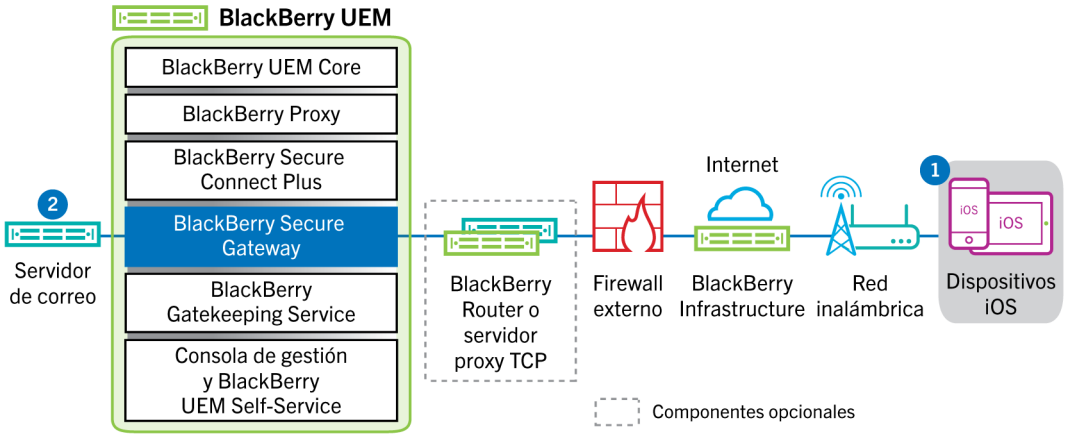
Este flujo de datos describe cómo se desplazan los datos del correo y del calendario de trabajo de dispositivos iOS al servidor de Exchange ActiveSync mediante BlackBerry Secure Gateway.



1. El usuario crea un mensaje de correo o actualiza un elemento del organizador en el espacio de trabajo.
2. El dispositivo envía el elemento nuevo o modificado a través de BlackBerry Infrastructure y BlackBerry Secure Gateway al servidor de correo.
3. El servidor de correo actualiza los datos del organizador en el buzón de correo del usuario o envía el elemento de correo al destinatario y envía una confirmación al dispositivo.

Flujo de datos: recepción de correo en un dispositivo iOS con BlackBerry Secure Gateway

Este flujo de datos describe cómo se desplazan los datos del correo y del calendario de trabajo entre dispositivos iOS y el servidor Exchange ActiveSync mediante BlackBerry Secure Gateway.

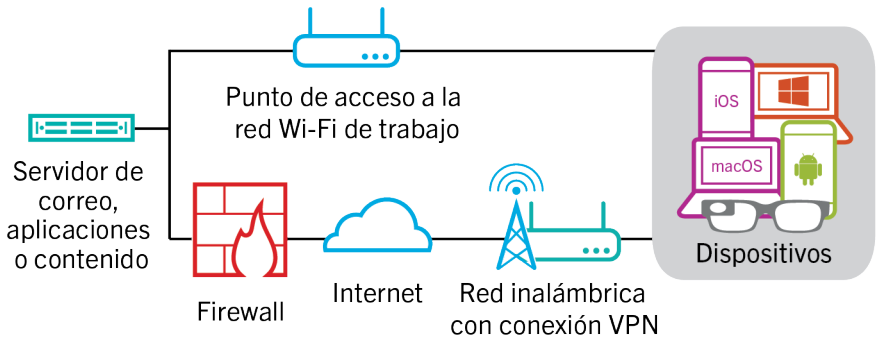


1. El cliente de correo electrónico nativo en iOS mantiene una conexión permanente con el servidor de correo a través de un canal cifrado y autenticado entre BlackBerry Infrastructure y BlackBerry Secure Gateway, y detecta los cambios en las carpetas configuradas para la sincronización en el servidor de correo.
2. Si hay elementos nuevos o modificados para el dispositivo, por ejemplo, un mensaje de correo electrónico nuevo o una entrada del calendario actualizada, el servidor de correo envía las actualizaciones al dispositivo a través del canal seguro establecido entre BlackBerry Secure Gateway y BlackBerry Infrastructure a la aplicación de correo electrónico y de organizador mediante el protocolo Exchange ActiveSync.

Envío y recepción de datos de trabajo mediante una VPN o red Wi-Fi de trabajo

Es posible que los dispositivos que tienen perfiles VPN o Wi-Fi configurados por usted u otro usuario puedan obtener acceso a los recursos de la empresa a través de la VPN de la empresa o la red Wi-Fi del trabajo. Para utilizar la VPN de la empresa, los usuarios con un dispositivo con Android que tenga el tipo de activación de Controles de MDM o Samsung Knox Workspace, deberán configurar manualmente un perfil de VPN en sus dispositivos.

Este diagrama muestra cómo se desplazan los datos cuando un dispositivo se conecta a los recursos de la empresa mediante la VPN de la empresa o la red Wi-Fi del trabajo.

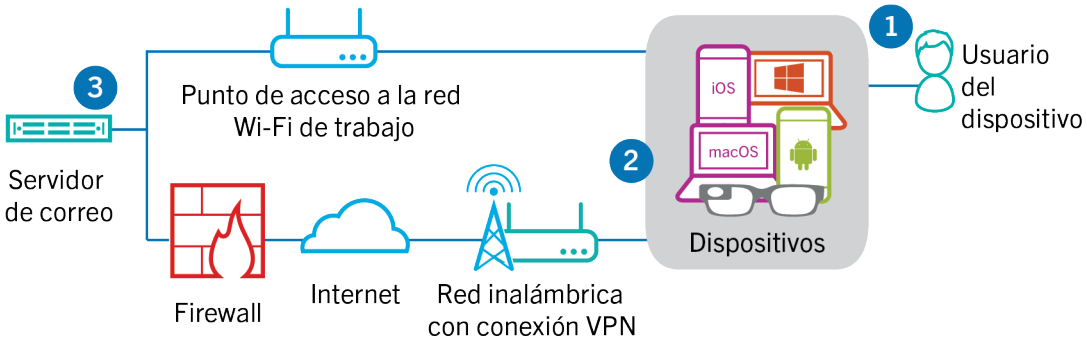


La siguiente tabla describe cuándo la red VPN de la empresa o la red Wi-Fi de trabajo utilizan dispositivos para conectarse a la red de su empresa.

Tipo de dispositivo	Descripción
Dispositivos con Android Enterprise y dispositivos con Knox Workspace	De forma predeterminada, los dispositivos con Android Enterprise y Knox Workspace utilizan la VPN de la empresa o la red Wi-Fi del trabajo para enviar y recibir datos de trabajo solo cuando BlackBerry Secure Connect Plus no está activado.
Dispositivos Windows y macOS, y dispositivos Android con el tipo de activación Controles de MDM	Los dispositivos Windows y macOS, y los dispositivos Android con el tipo de activación Controles de MDM utilizan la VPN de su empresa o la red Wi-Fi de trabajo para enviar y recibir datos de trabajo. Para utilizar la VPN de la empresa, los usuarios de los dispositivos Android deben configurar manualmente un perfil VPN en sus dispositivos.
iOS	Los dispositivos iOS utilizan la VPN de su empresa o la red Wi-Fi de trabajo para enviar y recibir datos de Exchange ActiveSync si BlackBerry Secure Gateway no está activado. El resto de datos de trabajo utilizan la red VPN de su empresa o la red Wi-Fi de trabajo.

Flujo de datos: envío de correo desde un dispositivo mediante una red VPN o una red Wi-Fi de trabajo

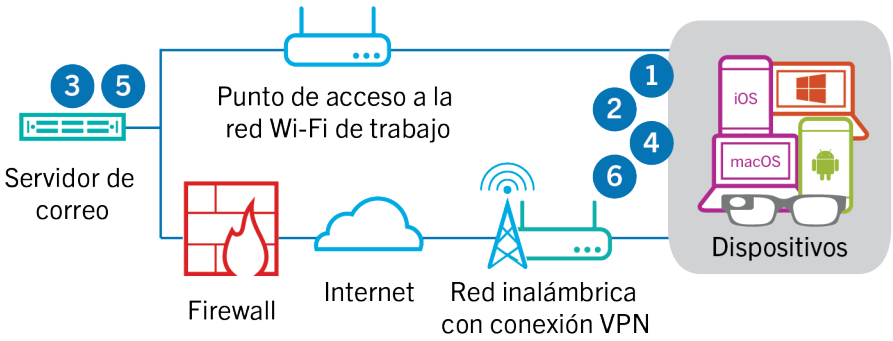
Este flujo de datos describe cómo se desplazan los datos del correo electrónico del trabajo y los datos del calendario desde el dispositivo al servidor de correo a través de la VPN o la red Wi-Fi de trabajo de la empresa mediante Exchange ActiveSync.



1. El usuario crea un mensaje de correo o actualiza un elemento del organizador en el espacio de trabajo.
2. El dispositivo envía el elemento nuevo o modificado al servidor de correo electrónico a través de la VPN o la red Wi-Fi de trabajo de la empresa.
3. El servidor de correo actualiza los datos del organizador en el buzón de correo del usuario o envía el elemento de correo al destinatario y envía una confirmación al dispositivo.

Flujo de datos: recepción de correo en un dispositivo mediante una red VPN o una red Wi-Fi de trabajo

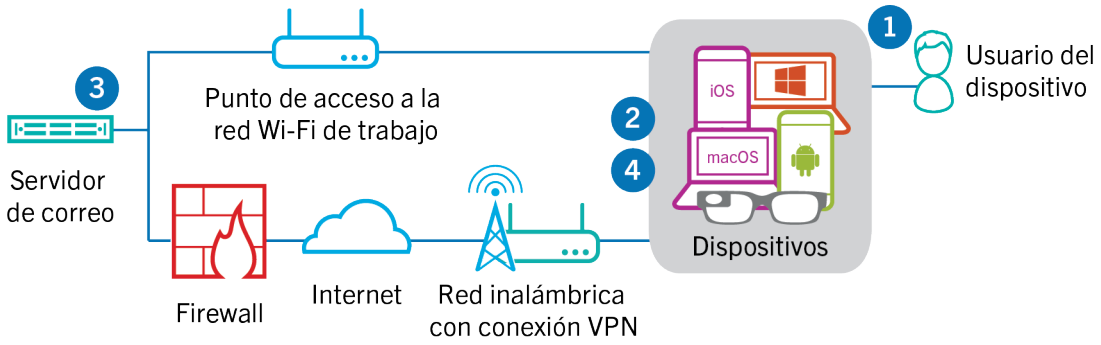
Este flujo de datos describe cómo se desplazan los datos del correo electrónico del trabajo y los datos del calendario desde el dispositivo al servidor de correo a través de la VPN o la red Wi-Fi de trabajo de la empresa mediante Exchange ActiveSync.



1. El dispositivo envía una solicitud HTTPS al servidor de correo y solicita que el servidor de correo notifique al dispositivo en el caso de que se modifique cualquier elemento en las carpetas que están configuradas para su sincronización. La solicitud se desplaza a través de la VPN de la empresa o red Wi-Fi del trabajo hasta el servidor de correo.
2. El dispositivo permanece en espera.
3. Cuando hay elementos nuevos o modificados para el dispositivo, por ejemplo, un mensaje de correo electrónico nuevo o una entrada actualizada del calendario, el servidor de correo envía las actualizaciones al dispositivo. Los elementos nuevos o modificados se desplazan a través de la VPN de la empresa o red Wi-Fi de trabajo a la aplicación de correo electrónico o de datos del dispositivo en el dispositivo.
4. Cuando la sincronización finaliza, el dispositivo envía otra solicitud para comenzar de nuevo el proceso.
5. Si no hay elementos nuevos ni modificados durante este intervalo, el servidor de correo o de aplicaciones envía un mensaje al dispositivo mediante el protocolo de Exchange ActiveSync.
6. El dispositivo envía una nueva solicitud y el proceso comienza de nuevo.

Flujo de datos: acceso a un servidor de aplicaciones o de contenido mediante una red VPN o una red Wi-Fi de trabajo

Este flujo de datos describe cómo se transfieren los datos entre un servidor de aplicaciones o de contenido de la empresa y una aplicación en un dispositivo a través de una conexión VPN o la red Wi-Fi de trabajo.



1. El usuario abre una aplicación de trabajo para ver los datos de trabajo. Por ejemplo, el usuario abre el navegador de trabajo para desplazarse por la intranet o utiliza una aplicación desarrollada de forma interna para acceder a los datos de los clientes de la empresa.
2. La aplicación establece una conexión con el servidor de aplicaciones o de contenido para recuperar los datos. La solicitud se desplaza a través de la VPN o red Wi-Fi de trabajo de la empresa hasta el servidor de aplicaciones o de contenido.
3. El servidor de aplicaciones o de contenido responde con los datos de trabajo. Los datos del trabajo se desplazan a través de la VPN o red Wi-Fi de trabajo a la aplicación en el espacio de trabajo del dispositivo.
4. La aplicación recibe y muestra los datos en el dispositivo.

Recepción de actualizaciones de configuración del dispositivo

Cuando se utiliza la consola de administración para enviar comandos del dispositivo como, por ejemplo, bloquear el dispositivo o eliminar datos de trabajo, o cuando se llevan a cabo otras tareas de administración del dispositivo, por ejemplo, la actualización de políticas, perfiles y configuración o asignación de aplicaciones, se desencadena una actualización de configuración para el dispositivo.

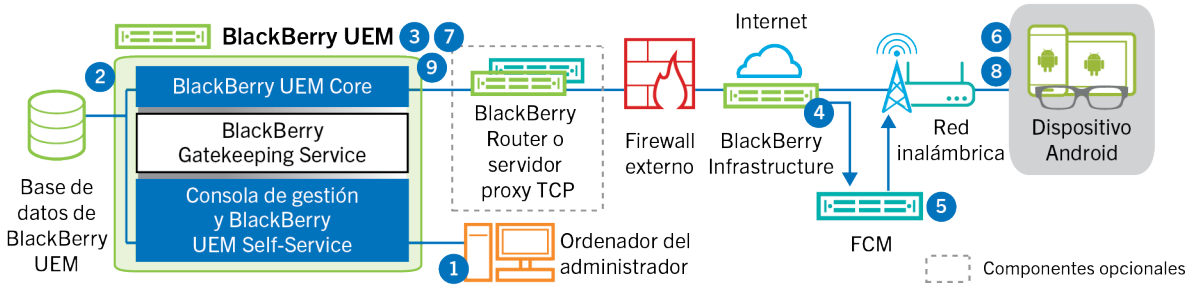
Cuando es necesario enviar una actualización de configuración a un dispositivo, BlackBerry UEM notifica al dispositivo que tiene una actualización de configuración pendiente. Los dispositivos también sondean BlackBerry UEM periódicamente para saber qué acciones deben ejecutarse en el dispositivo con el fin de evitar la pérdida de cualquier actualización de configuración en el caso de no recibir la notificación en el dispositivo.

En dispositivos con Android, BlackBerry UEM Client recibe y lleva a cabo todas las actualizaciones de configuración.

En dispositivos iOS, la aplicación BlackBerry UEM Client muestra el estado de conformidad y la información de configuración del dispositivo como, por ejemplo, las aplicaciones o políticas que se le han asignado. Sin embargo, el MDM Daemon nativo del dispositivo recibe y completa todas las actualizaciones de configuración enviadas al dispositivo.

En los dispositivos Windows 10 y macOS, que no requieren BlackBerry UEM Client para su activación, el MDM Daemon nativo recibe y completa todas las actualizaciones de configuración enviadas al dispositivo.

Flujo de datos: recepción de actualizaciones de configuración en un dispositivo Android



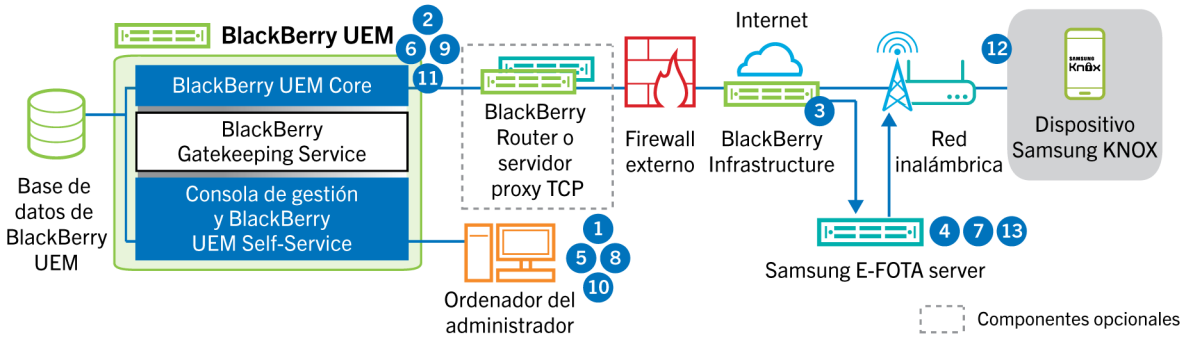
1. Se lleva a cabo una acción en la consola de gestión que desencadena una actualización de la configuración de un dispositivo Android.
2. Las actualizaciones se aplican en BlackBerry UEM y se identifican los objetos que se deben compartir con el dispositivo.
3. BlackBerry UEM Core se pone en contacto con BlackBerry Infrastructure a través de BlackBerry Router o del servidor proxy TCP, si está instalado, y del firewall externo a través del puerto 3101.
4. BlackBerry Infrastructure utiliza el servicio FCM para notificar a los dispositivos Android que hay una actualización pendiente.
5. El GCM envía una notificación a BlackBerry UEM Client en el dispositivo Android para que se ponga en contacto con BlackBerry UEM Core.
6. BlackBerry UEM Client se pone en contacto con BlackBerry UEM Core, a través del puerto 3101 en el firewall externo, para solicitar las acciones pendientes y los comandos que se deben implementar en el dispositivo.
7. BlackBerry UEM Core responde, a través de BlackBerry Infrastructure y BlackBerry Router o el servidor proxy TCP, si está instalado, con la acción de mayor prioridad.

   Se da prioridad a los comandos de administración de TI, tales como Eliminar datos del dispositivo y Bloquear dispositivo, seguido de las solicitudes de información del dispositivo, aplicaciones instaladas y así sucesivamente. BlackBerry UEM Core solo envía un comando a la vez. Si es necesario, se incluye información adicional en la respuesta.
8. BlackBerry UEM Client inspecciona la respuesta, programa el comando para que se procese y espera a que el comando se ejecute. BlackBerry UEM Client envía una respuesta a BlackBerry UEM Core, a través de BlackBerry Infrastructure, para actualizar el estado del comando. El estado indica si el comando se ha ejecutado correctamente y proporciona un mensaje de error en caso de fallo.
9. Si hay más acciones o comandos pendientes para el dispositivo, BlackBerry UEM Core responde a través de BlackBerry Infrastructure con la acción de más prioridad. Si no hay acciones ni comandos pendientes para el dispositivo, BlackBerry UEM Core responde con un comando inactivo.

   Los pasos del 7 al 9 se repiten hasta que no haya más acciones o comandos pendientes que se deban llevar a cabo en el dispositivo.

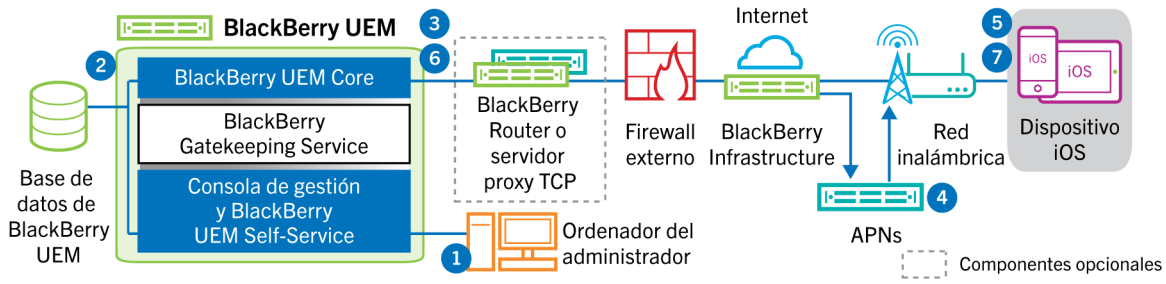
Flujo de datos: actualización del firmware en dispositivos Samsung Knox

Este flujo de datos describe el modo en que los datos se desplazan cuando utiliza Samsung Enterprise Firmware Over the Air para controlar el momento en que las actualizaciones de firmware de Samsung se instalan en los dispositivos. Para obtener más información, consulte Control de las versiones de software instaladas en los dispositivos en el contenido referente a Administración.



1. Un administrador puede agregar el ID de cliente y la clave de licencia de E-FOTA Samsung a BlackBerry UEM.
2. BlackBerry UEM Core envía la información de la licencia a BlackBerry Infrastructure a través de una conexión TLS.
3. BlackBerry Infrastructure Establece una conexión TLS con los servidores E-FOTA de Samsung y ofrece el ID y la clave de licencia del cliente.
4. El servidor de E-FOTA verifica la información y devuelve la información de la licencia mediante BlackBerry Infrastructure a BlackBerry UEM Core.
5. Un administrador puede crear un perfil de requisitos de versión de software del dispositivo y especificar el modelo del dispositivo de Samsung, el idioma y un proveedores de servicios inalámbricos para una nueva regla de firmware de dispositivos Samsung.
6. BlackBerry UEM Core se conecta al servidor E-FOTA por medio de BlackBerry Infrastructure a través de una conexión TLS y envía los criterios especificados al servidor E-FOTA.
7. El servidor de E-FOTA verifica la información y devuelve la información de mediante BlackBerry Infrastructure a BlackBerry UEM Core.
8. El administrador guarda el nuevo perfil de requisitos de informe especial del dispositivo.
9. BlackBerry UEM Core se conecta al servidor E-FOTA por medio de BlackBerry Infrastructure a través de una conexión TLS y envía el perfil a Samsung Cloud.
10. El administrador asigna el perfil de requisitos de informe especial del dispositivo a uno o varios usuarios.
11. BlackBerry UEM envía el perfil a BlackBerry UEM Client en el dispositivo Samsung del usuario.
12. El dispositivo Samsung se registra con el servidor E-FOTA.
13. Si hay disponible una actualización de firmware que cumpla con los parámetros especificados en el perfil de requisitos de informe especial del dispositivo, el servidor E-FOTA envía la actualización al dispositivo.

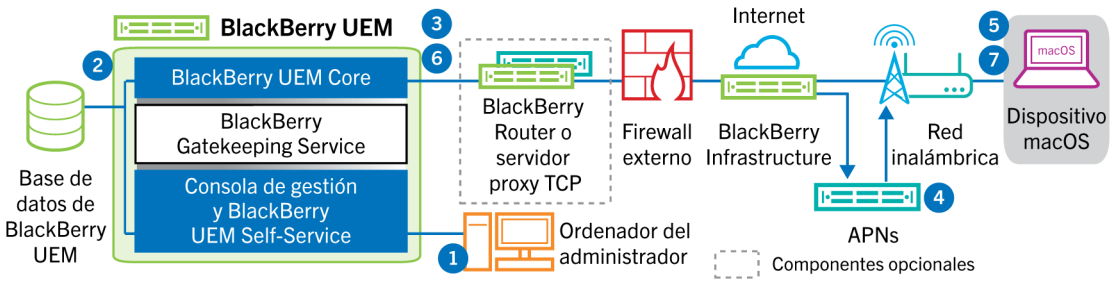
Flujo de datos: recepción de actualizaciones de configuración en un dispositivo iOS



1. Se lleva a cabo una acción en la consola de gestión que desencadena una actualización de la configuración de un dispositivo iOS. Por ejemplo, actualizar la política de TI o asignar un nuevo perfil o aplicación a la cuenta del usuario.
2. Las actualizaciones se aplican en BlackBerry UEM y se identifican los objetos que se deben compartir con el dispositivo.
3. BlackBerry UEM Core realiza las siguientes acciones:
   a. Se pone en contacto con BlackBerry Infrastructure a través de BlackBerry Router o del servidor proxy TCP, si está instalado, y del firewall externo a través del puerto 3101.
   b. Envía una solicitud a través de BlackBerry Infrastructure a los APN para notificar al dispositivo que hay una actualización pendiente.
4. El APN envía una notificación al MDM Daemon nativo en el dispositivo iOS para que se ponga en contacto con BlackBerry UEM Core.
5. Cuando el MDM Daemon nativo en el dispositivo iOS recibe la notificación, se pone en contacto con BlackBerry UEM Core, a través del puerto 3101 en el firewall externo, pasando a través de BlackBerry Router o el servidor proxy TCP, si está instalado, para recuperar las acciones pendientes.
6. BlackBerry UEM Core responde con la acción de mayor prioridad. Se da prioridad a las acciones del dispositivo como, por ejemplo, Eliminar datos del dispositivo y Bloquear dispositivo. BlackBerry UEM Core solo envía un comando a la vez. Si es necesario, se incluye información adicional en la respuesta. Si no hay acciones ni comandos pendientes para el dispositivo, BlackBerry UEM Core responde al dispositivo con un comando inactivo.
7. El MDM Daemon nativo en el dispositivo iOS realiza las siguientes acciones:
   a. Inspecciona la respuesta de BlackBerry UEM Core, programa el comando para que se procese y espera a que el comando se ejecute.
   b. Envía una respuesta a BlackBerry UEM Core para que actualice el estado del comando. El estado indica si el comando se ha ejecutado correctamente y proporciona un mensaje de error en caso de fallo.

   Los pasos 6 y 7 se repiten hasta que no haya más acciones o comandos pendientes que se deban llevar a cabo en el dispositivo.

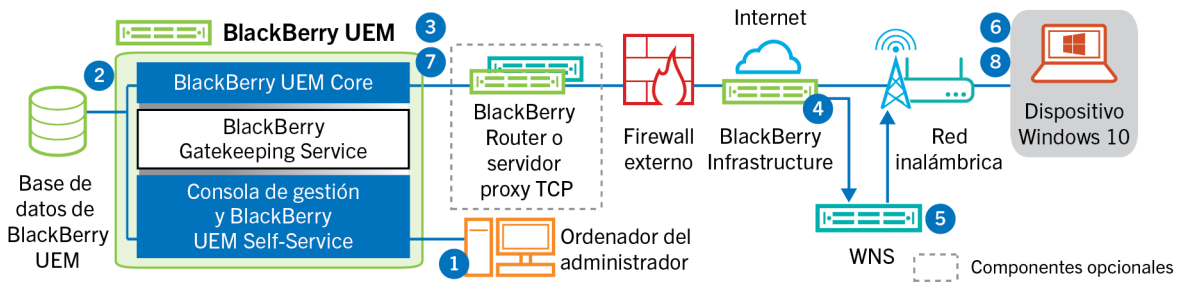
Flujo de datos: recepción de actualizaciones de configuración en un dispositivo macOS



1. Se lleva a cabo una acción en la consola de gestión que desencadena una actualización de la configuración de un dispositivo macOS. Por ejemplo, actualizar la política de TI o asignar un nuevo perfil o aplicación a la cuenta del usuario.
2. Las actualizaciones se aplican en BlackBerry UEM y se identifican los objetos que se deben compartir con el dispositivo.
3. BlackBerry UEM Core realiza las siguientes acciones:
   a. Se pone en contacto con BlackBerry Infrastructure a través de BlackBerry Router o del servidor proxy TCP, si está instalado, y del firewall externo a través del puerto 3101.
   b. Envía una solicitud a través de BlackBerry Infrastructure a los APN para notificar al dispositivo que hay una actualización pendiente.
4. Los APN envían una notificación al dispositivo para que se ponga en contacto con BlackBerry UEM Core.
5. Cuando el dispositivo recibe la notificación, se pone en contacto con BlackBerry UEM Core, a través del puerto 3101 en el firewall externo, pasando a través de BlackBerry Router o el servidor proxy TCP, si está instalado, para recuperar las acciones pendientes.
6. Cuando una actualización está pendiente para el dispositivo, BlackBerry UEM Core responde con la acción de mayor prioridad. Se da prioridad a las acciones del dispositivo como, por ejemplo, Eliminar datos del dispositivo y Bloquear dispositivo. Si es necesario, se incluye información adicional en la respuesta. Si no hay acciones ni comandos pendientes para el dispositivo, BlackBerry UEM Core responde al dispositivo con un mensaje vacío.
7. El dispositivo realiza las siguientes acciones:
   a. Inspecciona la respuesta de BlackBerry UEM Core, programa el comando para que se procese y espera a que el comando se ejecute.
   b. Envía una respuesta a BlackBerry UEM Core para que actualice el estado del comando. El estado indica si el comando se ha ejecutado correctamente y proporciona un mensaje de error en caso de fallo.

   Los pasos 6 y 7 se repiten hasta que no haya más acciones o comandos pendientes que se deban llevar a cabo en el dispositivo.

Flujo de datos: recepción de actualizaciones de configuración en un dispositivo Windows 10



1. Se lleva a cabo una acción en la consola de gestión que desencadena una actualización de la configuración de un dispositivo Windows 10. Por ejemplo, actualizar la política de TI o asignar un nuevo perfil o aplicación a la cuenta del usuario.
2. Las actualizaciones se aplican en BlackBerry UEM y se identifican los objetos que se deben compartir con el dispositivo.
3. BlackBerry UEM Core se pone en contacto con BlackBerry Infrastructure a través de BlackBerry Router o del servidor proxy TCP, si está instalado, y del firewall externo a través del puerto 3101.
4. BlackBerry Infrastructure utiliza el WNS para notificar al dispositivo que hay una actualización pendiente.
5. El WNS envía una notificación al dispositivo para que se ponga en contacto con BlackBerry UEM Core.
6. Cuando el dispositivo recibe la notificación, se pone en contacto con BlackBerry UEM Core, a través del puerto 3101 en el firewall externo, pasando a través de BlackBerry Router o el servidor proxy TCP, si está instalado, para recuperar las acciones pendientes.
7. Cuando una actualización está pendiente para el dispositivo, BlackBerry UEM Core responde con la acción de mayor prioridad. Se da prioridad a las acciones del dispositivo como, por ejemplo, Eliminar datos del dispositivo y Bloquear dispositivo. Si es necesario, se incluye información adicional en la respuesta. Si no hay acciones ni comandos pendientes para el dispositivo, BlackBerry UEM Core responde al dispositivo con un mensaje vacío.
8. El dispositivo inspecciona la respuesta, programa el comando para que se procese y espera a que el comando se ejecute. El dispositivo envía una respuesta a BlackBerry UEM Core para que actualice el estado del comando. El estado indica si el comando se ha ejecutado correctamente y proporciona un mensaje de error en caso de fallo.

   Los pasos 7 y 8 se repiten hasta que no haya más acciones o comandos pendientes para el dispositivo.

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