BlackBerry UEM

Descripción general y arquitectura

12.20

Contents

¿En qué consiste BlackBerry UEM? 5
Características principales de BlackBerry UEM 6
Características principales para todos los tipos de dispositivos 8
Características principales de cada tipo de dispositivo 11
Características compatibles por tipo de dispositivo 17

Arquitectura de BlackBerry UEM 22
Componentes BlackBerry UEM locales 27
Instalación distribuida local de BlackBerry UEM 30

Productos y servicios complementarios 34
Aplicaciones empresariales y BlackBerry Dynamics 34
Ventajas de BlackBerry Enterprise Identity 36
Ventajas de BlackBerry 2FA 36
Ventajas de BlackBerry Workspaces 36
Ventajas de BlackBerry UEM Notifications 37
SDK de empresa BlackBerry 37

Flujos de datos: activación de dispositivos y aplicaciones de BlackBerry Dynamics 39
Flujo de datos: activación de un dispositivo con Android Enterprise Trabajo y personal: privacidad de usuario mediante una cuenta de Google Play gestionada 39
Flujo de datos: activación de un dispositivo con Android Enterprise Trabajo y personal: control total mediante una cuenta de Google Play gestionada 41
Flujo de datos: activación de un dispositivo con Android Enterprise Solo espacio de trabajo mediante una cuenta de Google Play gestionada 42
Flujo de datos: activación de un dispositivo con Android Enterprise Trabajo y personal: privacidad de usuario en un dominio de Google 44
Flujo de datos: activación de un dispositivo con Android Enterprise Trabajo y personal: control total en un dominio de Google 45
Flujo de datos: activación de un dispositivo con Android Enterprise Solo espacio de trabajo en un dominio de Google 47
Flujo de datos: activación de un dispositivo para que utilice Knox Workspace 49
Flujo de datos: activación de un dispositivo iOS 50
Flujo de datos: activación de un dispositivo macOS 53
Flujo de datos: activación de un dispositivo Windows 10 54
Flujo de datos: activación de una aplicación de BlackBerry Dynamics por primera vez en un dispositivo 56
Flujo de datos: activación de una aplicación de BlackBerry Dynamics cuando ya hay una activada en el dispositivo 57

Flujo de datos: envío y recepción de datos de trabajo 58
Envío y recepción de datos de trabajo mediante BlackBerry Infrastructure 59

Flujo de datos: envío y recepción de datos de trabajo desde una aplicación de BlackBerry Dynamics mediante BlackBerry Dynamics NOC.....60
Flujo de datos: envío y recepción de datos de trabajo desde una aplicación de BlackBerry Dynamics mediante BlackBerry Infrastructure.....61
Flujo de datos: envío y recepción de datos de trabajo desde una aplicación de BlackBerry Dynamics mediante BlackBerry Dynamics Direct Connect.....61
Flujo de datos: acceso a un servidor de aplicaciones o contenido mediante BlackBerry Secure Connect Plus.....62
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.....63
Flujo de datos: autenticación con el servidor de correo desde un dispositivo con iOS cuando se usa BlackBerry Secure Gateway.....64
Flujo de datos: envío de correo desde un dispositivo iOS con BlackBerry Secure Gateway.....65
Flujo de datos: recepción de correo en un dispositivo iOS con BlackBerry Secure Gateway.....66
Envío y recepción de datos de trabajo mediante una VPN o red Wi-Fi de trabajo.....67
Flujo de datos: envío de correo desde un dispositivo mediante una red VPN o una red Wi-Fi de trabajo.....67
Flujo de datos: recepción de correo en un dispositivo mediante una red VPN o una red Wi-Fi de trabajo.....68
Flujo de datos: acceso a un servidor de aplicaciones o de contenido mediante una red VPN o una red Wi-Fi de trabajo.....69

Flujos de datos: recepción de actualizaciones de configuración del dispositivo.....70
Flujo de datos: recepción de actualizaciones de configuración en un dispositivo Android.....71
Flujo de datos: actualización del firmware en dispositivos Samsung Knox.....72
Flujo de datos: recepción de actualizaciones de configuración en un dispositivo iOS.....73
Flujo de datos: recepción de actualizaciones de configuración en un dispositivo macOS.....74
Flujo de datos: recepción de actualizaciones de configuración en un dispositivo Windows 10.....74

Aviso legal.....76

¿En qué consiste BlackBerry UEM?

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

Puede instalar UEM en un entorno local para obtener el máximo control sobre los servidores, los datos y los dispositivos, o puede utilizar UEM Cloud, que proporciona una solución segura, económica y fácil de utilizar. BlackBerry aloja UEM Cloud a través de Internet, por lo que solo necesita un navegador web compatible para acceder al servicio.

Tanto UEM local como UEM Cloud ofrecen seguridad integral de confianza y proporcionan el control que las empresas necesitan para gestionar todos los extremos y modelos de propiedad.

Entre las ventajas de UEM, se incluyen:

Función	Ventaja
Bajo coste total de propiedad	UEM local reduce la complejidad, optimiza los recursos agrupados, garantiza el máximo tiempo de actividad y le ayuda a alcanzar el menor coste total de propiedad para una solución local. UEM Cloud reduce los costes de propiedad al eliminar la necesidad de instalar, gestionar y actualizar los servicios.
Una sola interfaz basada en web	Gestione dispositivos iOS, macOS, Android y Windows, además de servicios adicionales, desde una única consola de administración.
Modelos de propiedad flexibles	Utilice un conjunto de políticas y perfiles personalizables para gestionar los dispositivos BYOD, COPE y COBO, y proteger la información empresarial.
Informes de usuario y dispositivo	Gestione grupos de dispositivos mediante informes y paneles completos, filtros dinámicos y capacidades de búsqueda.
Configuración e inscripción de usuarios sencillas	Permita a los usuarios que activen sus propios dispositivos en UEM con BlackBerry UEM Self-Service.
Seguridad móvil líder del sector	Saque el máximo partido a BlackBerry Infrastructure para garantizar la seguridad de los datos en todos los dispositivos.
Alta disponibilidad	Configure una alta disponibilidad local para minimizar las interrupciones del servicio para los usuarios de dispositivos o confíe en BlackBerry para mantener UEM Cloud y maximizar su tiempo de actividad.
Servicios adicionales disponibles	Active servicios como BlackBerry Workspaces, BlackBerry Enterprise Identity, BlackBerry 2FA, BBM Enterprise y Notificaciones UEM para añadir valor a su implementación de UEM.

Características principales de BlackBerry UEM

Función	Descripción
Administración de dispositivos multiplataforma	Puede administrar dispositivos con iOS, macOS, Android y Windows.
Interfaz de usuario única e intuitiva	Puede ver todos los dispositivos en un solo lugar y obtener acceso a todas las tareas de administración en una única interfaz de usuario basada en web. Puede compartir las labores con otros administradores que puedan acceder a la consola de administración al mismo tiempo. Se puede alternar entre las vistas predeterminada y avanzada para consultar las opciones de visualización de información y filtrar la lista de usuarios.
Experiencia segura y fiable	Los controles de dispositivos le ofrecen una administración precisa de la forma en que se conectan los dispositivos a su red, las capacidades activadas y las aplicaciones disponibles. Tanto si los dispositivos son propiedad de la empresa como de los usuarios, puede proteger los datos de su organización.
Separación de las necesidades laborales y personales	Puede gestionar los dispositivos mediante las tecnologías Android Enterprise, Android Management y Samsung Knox, que están diseñadas para mantener la información personal y la del trabajo separadas y protegidas en los dispositivos. Si el dispositivo se pierde o se pone en peligro, podrá eliminar solo la información relacionada con el trabajo o toda la información del dispositivo.
Conectividad IP segura	Puede utilizar BlackBerry Secure Connect Plus para proporcionar un túnel IP seguro entre las aplicaciones del espacio de trabajo en dispositivos iOS y Android que utilizan un perfil de trabajo y la red de la organización. Este túnel proporciona a los usuarios acceso a los recursos de trabajo protegidos por el firewall de la empresa, lo que garantiza que los datos estén protegidos mediante protocolos IPv4 estándar (TCP y UDP) y cifrado integral.
Autoservicio de usuario sencillo	BlackBerry UEM Self-Service reduce las solicitudes de asistencia y reduce los costes de TI de la empresa, al tiempo que da a los usuarios la opción de administrar sus dispositivos de forma puntual. Mediante UEM Self-Service, los usuarios pueden activar o cambiar dispositivos, cambiar las contraseñas de los dispositivos de forma remota, eliminar datos de los dispositivos o bloquear los dispositivos perdidos o robados.
Integración con otros servicios de BlackBerry	Puede integrar UEM con BlackBerry Workspaces, BlackBerry Enterprise Identity y BlackBerry 2FA para añadir valor a la instancia de UEM de su empresa.
Administración de aplicaciones eficaz	UEM es una plataforma de administración de aplicaciones integral para todos los dispositivos. Se pueden implementar aplicaciones de las principales tiendas, incluidas App Store y Google Play.

Función	Descripción
Administración basada en funciones	Puede compartir las labores con otros administradores que puedan acceder a la consola de administración al mismo tiempo. Se pueden utilizar roles para definir las acciones que puede realizar un administrador y reducir los riesgos de seguridad, distribuir las responsabilidades del trabajo y aumentar la eficiencia. Puede utilizar las funciones predefinidas o bien crear sus propias funciones personalizadas.
Integración del directorio de la empresa	Puede utilizar la autenticación de usuario local integrada para acceder a la consola de administración y a la consola de autoservicio, o bien puede integrar UEM con Microsoft Active Directory, LDAP o los directorios Entra ID que utiliza en el entorno de su empresa. UEM es compatible con las conexiones a varios directorios. Puede crear cuentas de usuario en UEM utilizando datos de usuario del directorio y puede vincular grupos de directorios de la empresa con UEM para organizar a los usuarios de UEM de la misma forma en que se organizan en el directorio de la empresa. También puede activar la integración para grupos específicos en el directorio de la empresa para crear usuarios de UEM automáticamente. Si activa la integración, también puede configurar la extracción para eliminar datos de dispositivos o cuentas de usuario cuando los usuarios se eliminan de los grupos en el directorio de su empresa.
Migración	Puede migrar usuarios, dispositivos, grupos y otros datos desde una base de datos de origen de UEM local a una nueva instancia de UEM Cloud o local.
Integración con Cisco ISE	Cisco Identity Services Engine (ISE) es el software de administración de red que ofrece a las empresas la capacidad de controlar el acceso de los dispositivos a la red de trabajo (por ejemplo, permitir o denegar las conexiones VPN o Wi-Fi). Puede crear una conexión entre Cisco ISE y UEM local para que Cisco ISE pueda recuperar los datos de los dispositivos que se activan en UEM. Cisco ISE comprueba los datos del dispositivo para determinar si los dispositivos cumplen con las políticas de acceso de su empresa.
Implementación regional	Puede configurar las conexiones regionales para funciones de conectividad de la empresa mediante la implementación de una o más instancias de BlackBerry Connectivity Node en una región específica. Esto se conoce como un grupo de servidores. Cada BlackBerry Connectivity Node incluye BlackBerry Secure Connect Plus, BlackBerry Gatekeeping Service, BlackBerry Secure Gateway, BlackBerry Proxy y BlackBerry Cloud Connector. Puede asociar los perfiles de conectividad de la empresa y de correo con un grupo de servidores para que todos los usuarios que estén asignados a dichos perfiles utilicen una conexión regional específica con BlackBerry Infrastructure al utilizar componentes de BlackBerry Connectivity Node. La implementación de uno o más BlackBerry Connectivity Node en un grupo de servidores también permite una alta disponibilidad y equilibrio de carga.

Función	Descripción
Dispositivos accesorios	Puede activar y gestionar determinados dispositivos accesorios Android en UEM. Por ejemplo, puede gestionar Vuzix M300 Smart Glasses. Las gafas inteligentes proporcionan a los usuarios acceso manos libres a información visual como notificaciones, instrucciones paso a paso, imágenes y vídeo, y les permiten emitir comandos de voz, escanear códigos de barras y utilizar la navegación GPS. Ejemplos de capacidades de gestión UEM que se admiten: activación de dispositivos mediante código QR, políticas de TI, perfiles de Wi-Fi y VPN, gestión de aplicaciones y servicios de ubicación.
Integración con Microsoft Intune	Para dispositivos iOS y Android, si desea proteger datos en aplicaciones Microsoft 365 que utilizan las funciones MAM de Microsoft Intune, puede utilizar Intune para proteger los datos de la aplicación mientras utiliza UEM para administrar los dispositivos. Intune ofrece características de seguridad para proteger los datos de aplicaciones. Por ejemplo, Intune puede requerir que los datos de las aplicaciones se cifren e impidan copiar y pegar, imprimir y usar el comando Guardar como. Puede conectar UEM a Intune, lo que le permite gestionar políticas de protección de aplicaciones Intune desde dentro de la consola de gestión de UEM.

Características principales para todos los tipos de dispositivos

Función	Descripción
Activar dispositivos	Cuando un usuario activa un dispositivo, lo asocia con UEM y el entorno de su empresa para poder acceder a los datos de trabajo en el dispositivo. Los usuarios pueden activar sus dispositivos con un código QR o su dirección de correo electrónico y una contraseña de activación. Puede permitir a los usuarios que activen los dispositivos por su cuenta o bien puede activar los dispositivos para los usuarios y, a continuación, distribuirlos. Todos los tipos de dispositivo se pueden activar a través de la red inalámbrica.

Función	Descripción
Gestionar dispositivos	Puede ver todos los dispositivos y obtener acceso a todas las tareas de administración en una única consola basada en web. Puede administrar varios dispositivos para cada cuenta de usuario y ver el inventario de dispositivos de su empresa. Si el dispositivo las admite, pueden realizarse las acciones siguientes: • Bloquear el dispositivo, cambiar la contraseña del dispositivo o del espacio de trabajo o eliminar la información del dispositivo. • Conectar el dispositivo de forma segura al entorno de correo de la empresa, mediante Microsoft Exchange ActiveSync para la compatibilidad con el correo electrónico y el calendario. • Controlar el modo en que el dispositivo se puede conectar a la red de la empresa, incluida la configuración de Wi-Fi y de la VPN. • Configurar el inicio de sesión único para el dispositivo de modo que se autentique automáticamente con los dominios y servicios web en la red de su empresa. • Controlar las capacidades del dispositivo, tales como definir reglas para establecer la seguridad de la contraseña y desactivar funciones como la cámara. • Administrar la disponibilidad de las aplicaciones en el dispositivo, incluida la especificación de las versiones de las aplicaciones y si son necesarias u opcionales. • Buscar directamente en las tiendas de aplicaciones las aplicaciones que se van a asignar a los dispositivos. • Instalar los certificados en el dispositivo y, opcionalmente, configurar SCEP para permitir la inscripción automática de certificados. • Ampliar la seguridad del correo electrónico mediante S/MIME o PGP.
Gestión de grupos de usuarios, aplicaciones y dispositivos	Los grupos simplifican la gestión de usuarios, aplicaciones y dispositivos. Puede usar grupos para aplicar los mismos valores de configuración a cuentas de usuario o dispositivos similares. Puede asignar diferentes grupos de aplicaciones a diferentes grupos de usuarios y un usuario puede ser miembro de varios grupos.
Control de los dispositivos que pueden acceder a Microsoft Exchange ActiveSync	El uso de enlaces garantiza que solo los dispositivos administrados por UEM puedan acceder al correo electrónico del trabajo y al resto de información del dispositivo y cumplir con las políticas de seguridad de la empresa.
Controlar cómo se conectan las aplicaciones a los recursos de la empresa	Puede utilizar el perfil de conectividad de la empresa para controlar cómo se conectan las aplicaciones de los dispositivos con los recursos de la empresa. Al activar la conectividad de la empresa, evite tener que abrir puertos múltiples en el firewall de la empresa a Internet para la administración de dispositivos y aplicaciones de terceros como el servidor de correo, la autoridad de certificación y otros servidores web o servidores de contenido. La conectividad de la empresa envía todo el tráfico a través de BlackBerry Infrastructure a UEM en el puerto 3101.

Función	Descripción
Administrar las aplicaciones de trabajo	En todos los dispositivos administrados, las aplicaciones de trabajo son aplicaciones que la empresa pone a disposición de sus usuarios. Se pueden buscar directamente en las tiendas las aplicaciones que se van a asignar a los dispositivos. Puede especificar si las aplicaciones son necesarias en los dispositivos y puede ver si una aplicación de trabajo está instalada en el dispositivo. Las aplicaciones de trabajo también pueden ser aplicaciones propias desarrolladas por su empresa o por desarrolladores terceros para su uso en la empresa.
Aplique los requisitos de dispositivos de su empresa	Puede utilizar un perfil de conformidad para aplicar los requisitos de seguridad de la empresa; por ejemplo, no permitir el acceso a los datos de trabajo en los dispositivos en los que se ha realizado jailbreak (liberación) o root, o aquellos que tengan una alerta de integridad o que requieran que se instalen determinadas aplicaciones en el dispositivo. Puede enviar una notificación a los usuarios para pedirles que cumplan los requisitos de su empresa o puede limitar el acceso de los usuarios a los recursos y aplicaciones de su empresa, eliminar datos de trabajo o eliminar todos los datos del dispositivo.
Envío de un correo a los usuarios	Se puede enviar un correo a varios usuarios directamente desde la consola de gestión.
Crear o importar varias cuentas de usuario con un archivo .csv	Puede importar un archivo .csv a UEM para crear o importar varias cuentas de usuario al mismo tiempo. En función de sus necesidades, también puede especificar la pertenencia al grupo y la configuración de activación de las cuentas de usuario en el archivo .csv.
Ver informes de usuario e información sobre el dispositivo	El panel de control de informes muestra información general sobre su entorno de UEM. Por ejemplo, puede ver el número de dispositivos de la empresa ordenados por proveedor de servicios. Puede ver los detalles acerca de los usuarios y dispositivos, exportar la información a un archivo .csv, y acceder a las cuentas de usuario desde el panel.
Alta disponibilidad y recuperación de desastres	Los centros de datos de BlackBerry están ubicados en todo el mundo y se han diseñado para proporcionar una alta disponibilidad y recuperación de desastres. Los centros de datos de BlackBerry proporcionan un acceso físico seguro a edificios, así como supervisión y redundancia de hardware para ayudar a proteger los datos de la empresa frente a desastres naturales. Los centros de datos de BlackBerry cuentan con planes de recuperación frente a desastres en caso de interrupciones del suministro. Los planes están diseñados para tener un impacto mínimo en los usuarios y asegurar la continuidad del negocio. Las copias de seguridad de los datos y las aplicaciones se realizan casi en tiempo real para evitar la pérdida de datos.
Autenticación basada en certificados	Puede enviar certificados a los dispositivos mediante los perfiles de certificados. Estos perfiles ayudan a restringir el acceso a Microsoft Exchange ActiveSync y las conexiones Wi-Fi o conexiones VPN a los dispositivos que utilizan la autenticación basada en certificados.

Función	Descripción
Administrar licencias para características específicas y controles del dispositivo	Puede administrar las licencias y ver información detallada para cada tipo de licencia, por ejemplo, el uso y la fecha de caducidad. Los tipos de licencia que utiliza su empresa determinan los dispositivos y características que se pueden administrar. Debe activar las licencias para poder activar los dispositivos. Existen periodos de prueba gratuita para que pueda probar el servicio.

Características principales de cada tipo de dispositivo

Dispositivos iOS

Función	Descripción
Activación del dispositivo	Puede utilizar Apple Configurator 2 para preparar dispositivos para la activación con UEM. Los usuarios pueden activar dispositivos preparados sin utilizar BlackBerry UEM Client.
Filtro de contenido web	Puede utilizar perfiles de filtro de contenido web para limitar los sitios web que un usuario puede ver en un dispositivo. Puede activar el filtrado automático con la opción de permitir y restringir los sitios web o para permitir el acceso solo a determinados sitios web.
Vincular cuentas de Apple VPP a un dominio de UEM	El programa de compras por volumen (VPP) le permite adquirir y distribuir grandes cantidades de aplicaciones de iOS. Puede vincular cuentas de Apple VPP a un dominio de UEM de modo que sea posible distribuir licencias adquiridas para las aplicaciones iOS asociadas a las cuentas VPP.
Programa de inscripción de dispositivos de Apple	Puede configurar UEM para utilizar el programa de inscripción de dispositivos (DEP) de Apple para poder sincronizar UEM con DEP. Después de configurar UEM, puede utilizar la consola de administración para gestionar la activación de los dispositivos iOS que haya adquirido la empresa para el DEP. Puede utilizar varias cuentas de DEP. Puede enlazar varias cuentas de Apple DEP con un dominio de UEM.
Compatibilidad con soluciones PKI basadas en aplicación	UEM es compatible con soluciones PKI basadas en aplicación, como Purebred, que puede inscribir certificados para aplicaciones de BlackBerry Dynamics. Ahora puede instalar la aplicación PKI en dispositivos y permitir que las versiones más recientes de las aplicaciones de BlackBerry Dynamics, como BlackBerry Work y BlackBerry Access, utilicen certificados inscritos a través de la aplicación PKI.
Perfiles de carga personalizados	Se pueden utilizar perfiles de carga personalizados para controlar las funciones de dispositivos iOS que no están controladas por las políticas o perfiles de UEM. Puede crear perfiles de configuración de Apple mediante Apple Configurator y agregarlos a perfiles de carga personalizados de UEM. Se pueden asignar perfiles de carga personalizados a usuarios, grupos de usuarios y grupos de dispositivos.

Función	Descripción
BlackBerry Secure Gateway	BlackBerry Secure Gateway permite que los dispositivos iOS con el tipo de activación de controles de MDM se conecten al servidor de correo de trabajo a través de BlackBerry Infrastructure y UEM. Si utiliza BlackBerry Secure Gateway, no tendrá que exponer su servidor de correo fuera del firewall para permitir que los usuarios de estos dispositivos reciban correo de trabajo cuando no estén conectados a la VPN de la empresa o a la red Wi-Fi de trabajo.
Integración con BlackBerry Dynamics	También puede utilizar el perfil de BlackBerry Dynamics para permitir que los dispositivos iOS puedan acceder a las aplicaciones de productividad de BlackBerry Dynamics como BlackBerry Work, BlackBerry Access y BlackBerry Connect. Se puede asignar el perfil de BlackBerry Dynamics a cuentas de usuarios, a grupos de usuarios y a grupos de dispositivos. Varios dispositivos pueden acceder a las mismas aplicaciones. El perfil le permite activar BlackBerry Dynamics para los usuarios que no están aún activados en BlackBerry Dynamics.
VPN por aplicación	Puede configurar VPN por aplicación en los dispositivos iOS para especificar qué aplicaciones en los dispositivos deben utilizar una VPN para sus datos en tránsito. VPN por aplicación contribuye a disminuir la carga de la VPN de la empresa al permitir que solo parte del tráfico de trabajo utilice la VPN (por ejemplo, al acceder a servidores de aplicaciones o páginas web que están detrás del firewall). Esta característica también es compatible con la privacidad del usuario y aumenta la velocidad de conexión de las aplicaciones personales al no enviar el tráfico personal a través de la VPN. Para los dispositivos iOS, las aplicaciones se asocian a un perfil de VPN cuando asigna la aplicación o grupo de aplicaciones a un usuario, grupo de usuarios o grupo de dispositivos.
Bloqueo de activación de Apple	La función de bloqueo de activación requiere el ID de Apple y la contraseña del usuario para poder desactivar Buscar mi iPhone, borrar el dispositivo o reactivar y utilizar el dispositivo. Puede evitar el bloqueo de activación para proporcionar un dispositivo COPE o COBO a un usuario distinto.
Listas de aplicaciones personales	Puede ver una lista de aplicaciones que están instaladas en un espacio personal del usuario en dispositivos iOS de su entorno. Puede ver una lista de aplicaciones personales instaladas en el dispositivo de un usuario en la página de detalles del usuario o ver una lista de todas las aplicaciones personales instaladas en los espacios personales de los usuarios en la página de aplicaciones personales en la consola de administración.
Ejecución del modo de bloqueo de la aplicación	En dispositivos iOS supervisados mediante Apple Configurator 2, se puede usar un perfil de modo de bloqueo de aplicaciones para limitar el dispositivo y que solo se ejecute una aplicación. Por ejemplo, puede limitar el acceso a una sola aplicación con fines de formación o bien para realizar demostraciones en el punto de venta.
Modo perdido para dispositivos iOS supervisados	El modo perdido permite bloquear un dispositivo, definir un mensaje para que se muestre y ver la ubicación actual del dispositivo perdido. Puede activar el modo perdido para los dispositivos iOS supervisados.

Función	Descripción
Compatibilidad de IBM Notes Traveler	Los dispositivos con iOS se pueden conectar a IBM Notes Traveler mediante BlackBerry Secure Gateway.
Compatibilidad con Face ID	UEM es compatible con Face ID para la autenticación de dispositivos o para abrir aplicaciones de BlackBerry Dynamics.
Administración de dispositivos compartidos	Puede permitir que varios usuarios compartan un dispositivo iOS. Puede personalizar los términos de uso que los usuarios deben aceptar para desinscribir dispositivos compartidos. Un usuario puede desinscribir un dispositivo mediante autenticación local y, cuando termine de utilizarlo, inscribirlo para que esté disponible para el siguiente usuario. Los dispositivos gestionados siguen siendo gestionados por UEM durante el proceso de desinscripción e inscripción. Esta función se ha diseñado para dispositivos supervisados con la configuración siguiente: • Modo de bloqueo de la aplicación activado • Aplicaciones de VPP asignadas
iPad	Los dispositivos iPad se pueden compartir entre varios usuarios. Cuando los usuarios inician sesión con un ID administrado de Apple, sus datos se cargan y el usuario puede acceder a sus propias cuentas de correo electrónico, archivos, biblioteca de fotos iCloud, datos de aplicaciones y más.

Dispositivos Android

Función	Descripción
Administrar dispositivos Android Enterprise y Android Management	Puede activar dispositivos Android para utilizar Android Enterpriseo Android Management, que son funciones desarrolladas por Google y proporcionan seguridad adicional a las empresas que desean administrar y permitir las aplicaciones y los datos en los dispositivos Android. Los dispositivos se pueden activar para contar solo con un perfil de trabajo o para tener tanto perfiles de trabajo como personales. Puede tener el control total de ambos perfiles y la capacidad para eliminar todos los datos del dispositivo o puede permitir la privacidad de usuarios para perfiles personales y solo la capacidad de eliminar los datos de trabajo del dispositivo. Los dispositivos Samsung ofrecen opciones de administrador adicionales, como un conjunto mejorado de reglas de política de TI, cuando se activan con Android Enterprise.
Activaciones de Trabajo y personal: control total para dispositivos conAndroid Enterprise y Android Management	Este tipo de activación le permite administrar todo el dispositivo. Crea un perfil de trabajo en el dispositivo que separa los datos personales y de trabajo, pero permite que su empresa mantenga el control total sobre el dispositivo y borre todos los datos de este. Tanto los datos de los perfiles de trabajo como los personales estarán protegidos mediante cifrado y un método de autenticación, como una contraseña.

Función	Descripción
Administrar dispositivos mediante Knox MDM y Knox Workspace	UEM puede administrar los dispositivos con Samsung mediante Samsung Knox MDM y Samsung Knox Workspace. Knox Workspace proporciona un contenedor cifrado protegido mediante contraseña en un dispositivo Samsung que incluye sus aplicaciones y datos de trabajo. Separa las aplicaciones y los datos personales del usuario de las aplicaciones y los datos de la empresa y protege las aplicaciones y los datos de trabajo mediante las capacidades de seguridad y administración mejoradas que ha desarrollado Samsung. Cuando se activa un dispositivo, UEM identifica automáticamente si es compatible con Knox. Además de las funciones de administración estándar de Android, UEM incluye las siguientes funciones para los dispositivos compatibles con Knox: • Conjunto mejorado de reglas de política de TI • Administración de aplicaciones mejorada incluida la instalación y desinstalación de aplicaciones sin aviso, así como de la desinstalación sin aviso de aplicaciones restringidas y la prohibición de instalar aplicaciones restringidas • Modo de bloqueo de la aplicación Para obtener más información sobre los dispositivos compatibles, consulte la matriz de compatibilidad.
Integración con BlackBerry Dynamics	También puede utilizar el perfil de BlackBerry Dynamics para permitir que los dispositivos Android puedan acceder a las aplicaciones de productividad de BlackBerry Dynamics como BlackBerry Work, BlackBerry Access y BlackBerry Connect. Se puede asignar el perfil de BlackBerry Dynamics a cuentas de usuarios, a grupos de usuarios y a grupos de dispositivos. Varios dispositivos pueden acceder a las mismas aplicaciones. El perfil le permite activar BlackBerry Dynamics para los usuarios que no están aún activados en BlackBerry Dynamics.
VPN por aplicación	Puede activar una VPN por aplicación para dispositivos Android que utilizan un perfil de trabajo para restringir el uso de BlackBerry Secure Connect Plus para aplicaciones específicas del espacio de trabajo que agregue a una lista de permitidos.
Inscripción desatendida	UEM es compatible con dispositivos que tengan activada la inscripción desatendida. La inscripción desatendida ofrece un método de implementación optimizado para dispositivos Android que son propiedad de la empresa, lo que hace que la implementación de dispositivos a gran escala sea rápida, fácil y segura. La inscripción desatendida permite a los administradores configurar de forma sencilla dispositivos en línea y tener preparada la gestión forzada cuando los empleados reciben sus dispositivos. Para más información de Google, consulte Gestión de la inscripción desatendida y la descripción general de la inscripción desatendida. Puede empezar con la inscripción desatendida en unos pocos pasos: compre dispositivos, asigne los dispositivos a usuarios, configure políticas para su empresa e implemente los dispositivos para usuarios. Debe colaborar con su distribuidor u operador para obtener acceso al portal de inscripción desatendida y configurar los dispositivos en el portal.

Función	Descripción
Compatibilidad con soluciones PKI basadas en aplicación	UEM es compatible con soluciones PKI basadas en aplicación, como Purebred, que puede inscribir certificados para aplicaciones de BlackBerry Dynamics. Ahora puede instalar la aplicación PKI en dispositivos y permitir que las versiones más recientes de las aplicaciones de BlackBerry Dynamics, como BlackBerry Work y BlackBerry Access, utilicen certificados inscritos a través de la aplicación PKI.
SafetyNet y Play Integrity	Cuando los administradores activan la atestación Android SafetyNet o Google Play Integrity, UEM realiza comprobaciones para probar la autenticidad e integridad de los dispositivos Android que se han activado con los tipos de activación de Android Enterprise, Samsung Knox y de controles de MDM en el entorno de su empresa.
Cumplimiento del nivel de revisión de seguridad para las aplicaciones de BlackBerry Dynamics	Puede aplicar el cumplimiento del nivel de revisión de seguridad a las aplicaciones BlackBerry Dynamics. Si el nivel de revisión de seguridad no se cumple, puede eliminar los datos de la aplicación BlackBerry Dynamics, no permitir que las aplicaciones BlackBerry Dynamics se ejecuten en el dispositivo o no realizar ninguna acción en el dispositivo.
Credenciales inteligentes derivadas	Utilice las credenciales inteligentes derivadas de Entrust IdentityGuard para firmar, cifrar y autenticar aplicaciones de BlackBerry Dynamics, aplicaciones del espacio de trabajo de Android Enterprise y dispositivos con Samsung Knox Workspace.
Protección contra el restablecimiento de los datos de fábrica para dispositivos con Android Enterprise	Puede configurar un perfil de protección contra el restablecimiento de los datos de fábrica para los dispositivos con Android Enterprise de su empresa que se hayan activado mediante el tipo de activación Solo espacio de trabajo. Este perfil le permite especificar una cuenta de usuario que se puede utilizar para desbloquear un dispositivo después de que se haya restablecido a los valores predeterminados de fábrica o eliminar la necesidad de iniciar sesión después de que el dispositivo se haya restablecido a los valores predeterminados de fábrica.

Dispositivos Windows

Función	Descripción
Compatibilidad con dispositivos con Windows 10	Se pueden administrar los dispositivos Windows, incluidos los dispositivos móviles con Windows 10 y las tabletas y los equipos con Windows 10.
Compatibilidad de proxy para dispositivos Windows 10	Se pueden configurar conexiones de trabajo Wi-Fi y VPN para dispositivos Windows 10, y puede configurar un servidor proxy como parte del perfil de Wi-Fi de los dispositivos Windows 10 Mobile.

Función	Descripción
VPN por aplicación	Puede configurar VPN por aplicación en los dispositivos Windows 10 para especificar qué aplicaciones en los dispositivos deben utilizar una VPN para sus datos en tránsito. VPN por aplicación contribuye a disminuir la carga de la VPN de la empresa al permitir que solo parte del tráfico de trabajo utilice la VPN (por ejemplo, al acceder a servidores de aplicaciones o páginas web que están detrás del firewall). Esta característica también es compatible con la privacidad del usuario y aumenta la velocidad de conexión de las aplicaciones personales al no enviar el tráfico personal a través de la VPN.
Windows Information Protection para dispositivos con Windows 10	Puede configurar los perfiles de Windows Information Protection para separar los datos personales y del trabajo en los dispositivos, evitar que los usuarios compartan datos de trabajo fuera de las aplicaciones de trabajo protegidas o con personas de fuera de la empresa, y realizar auditorías de las prácticas inapropiadas de uso compartido de datos. Puede especificar qué aplicaciones están protegidas y son de confianza para crear y acceder a los archivos de trabajo.
Permitir los proveedores de antivirus	En el perfil de cumplimiento, en la regla "Estado del antivirus" para dispositivos con Windows, puede optar por permitir los programas de antivirus de cualquier proveedor o únicamente permitir aquellos que haya agregado a la lista de "Proveedores de antivirus permitidos". La regla se aplicará si un dispositivo tiene activado un programa antivirus de cualquier proveedor que no esté permitido.
Combinación de Entra ID	UEM es compatible con la combinación de Entra ID, que permite un proceso de inscripción a MDM simplificado para los dispositivos Windows 10. Los usuarios pueden inscribir sus dispositivos con UEM usando su nombre de usuario y contraseña de Entra ID. La combinación de Entra ID también requiere la compatibilidad con Windows 10 AutoPilot, que permite que los dispositivos Windows 10 puedan activarse de forma automática con UEM durante la experiencia de configuración inicial de Windows 10.

Dispositivos macOS

Función	Descripción
Administración básica de dispositivos mediante controles de dispositivos	Cuando un usuario activa un dispositivo macOS, el dispositivo y el usuario se configuran como entidades independientes en UEM. Se establecen canales de comunicación independientes entre UEM y el dispositivo y entre UEM y la cuenta de usuario, lo que le permite gestionar el dispositivo y el usuario por separado.
Perfiles y políticas.	Algunos perfiles solo se asignan al usuario (por ejemplo, los perfiles de correo). Algunos perfiles solo se asignan al dispositivo (por ejemplo, los perfiles de proxy). Algunos perfiles permiten elegir si el perfil debe aplicarse al dispositivo o al usuario (por ejemplo, los perfiles Wi-Fi). Puede controlar el dispositivo a través de comandos y políticas de TI. Los usuarios activan los dispositivos macOS mediante BlackBerry UEM Self-Service.

Características compatibles por tipo de dispositivo

Esta referencia rápida compara las capacidades compatibles de los dispositivos iOS, macOS, Android y Windows 10 en BlackBerry UEM.

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

Características del dispositivo

Función	iOS	macOS	Android	Windows 10
Activación inalámbrica	√	√	√	√
Activación inalámbrica mediante un código QR	√		√	
Aplicación de cliente necesaria para la activación	√ [1]		√	
Personalización del acuerdo de los términos de uso para la activación	√	√	√	√
Restricción de la activación por modelo de dispositivo	√	√	√	
Presentación y exportación del informe del dispositivo (p. ej., detalles de hardware)	√	√	√	√
Restringir los dispositivos sin supervisión	√ [2]	√ [2]		

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

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

Características de seguridad

Función	iOS	macOS	Android	Windows 10
Separación de los datos personales y de trabajo	√ [1]		√ [2]	√
Privacidad del usuario para los datos personales	√ [1]		√ [2]	
Cifrado de los datos de trabajo almacenados	√ [1]		√ [2]	√

Función	iOS	macOS	Android	Windows 10
Envío de comandos de TI a los dispositivos	√	√	√	√
Control de las capacidades del dispositivo mediante políticas de TI	√	√	√	√
Eliminación de los datos de trabajo tras un periodo de inactividad	√ [1]		√ [1]	
Aplicar los requisitos de la contraseña	√	√	√	√
Aplicar el cifrado de la tarjeta de memoria			√ [3]	
Aplicar el cifrado del almacenamiento interno			√	√

[1] Requiere las aplicaciones de BlackBerry Dynamics.

[2] Requiere las aplicaciones Samsung Knox Workspace, Android Enterprise, Android Management o BlackBerry Dynamics.

[3] Para los dispositivos Samsung Knox únicamente.

Envío de certificados a los dispositivos

Función	iOS	macOS	Android	Windows 10
Perfiles de certificado de CA	√	√	√	√
Perfiles SCEP	√	√	√	√
Perfiles de certificado compartido	√	√	√	
Perfiles de credenciales de usuario	√	√	√	

Administración de las conexiones de trabajo de los dispositivos

Función	iOS	macOS	Android	Windows 10
Perfiles de BlackBerry 2FA	√		√	
Perfiles de conectividad de BlackBerry Dynamics	√	√	√	√
Perfiles de CalDAV	√	√		

Función	iOS	macOS	Android	Windows 10
Perfiles de CardDAV	√	√		
Conectividad de la empresa				
BlackBerry Secure Connect Plus	√		√ [1]	
Perfiles de correo de Exchange ActiveSync	√	√	√ [2]	√
BlackBerry Secure Gateway	√			
Perfiles de correo IMAP/POP3	√	√	√	√
Perfiles de proxy	√	√	√	√
Perfiles de registro único	√			
Perfiles VPN	√	√	√ [3]	√
Perfiles de Wi-Fi	√	√	√	√

[1] Solo para dispositivos Android Enterprise y Knox Workspace.

[2] Solo para dispositivos Motorola que son compatibles con EDM API, dispositivos Android Enterprise y dispositivos Knox.

[3] Para los dispositivos Knox Workspace únicamente.

Gestión de los estándares de la empresa para dispositivos

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

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

Protección de dispositivos perdidos o robados

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

[1] Solo para dispositivos Android Enterprise.

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

Configuración de roaming

Función	iOS	macOS	Android	Windows 10
Desactivación de la sincronización automática cuando se encuentra en roaming	√		√ [1]	
Desactivación de datos cuando se encuentra en roaming	√ [2]		√ [3]	√

[1] Solo para dispositivos Knox.

[2] Puede configurar el roaming de datos en un perfil de uso de red.

[3] Solo para dispositivos Android Enterprise y Knox.

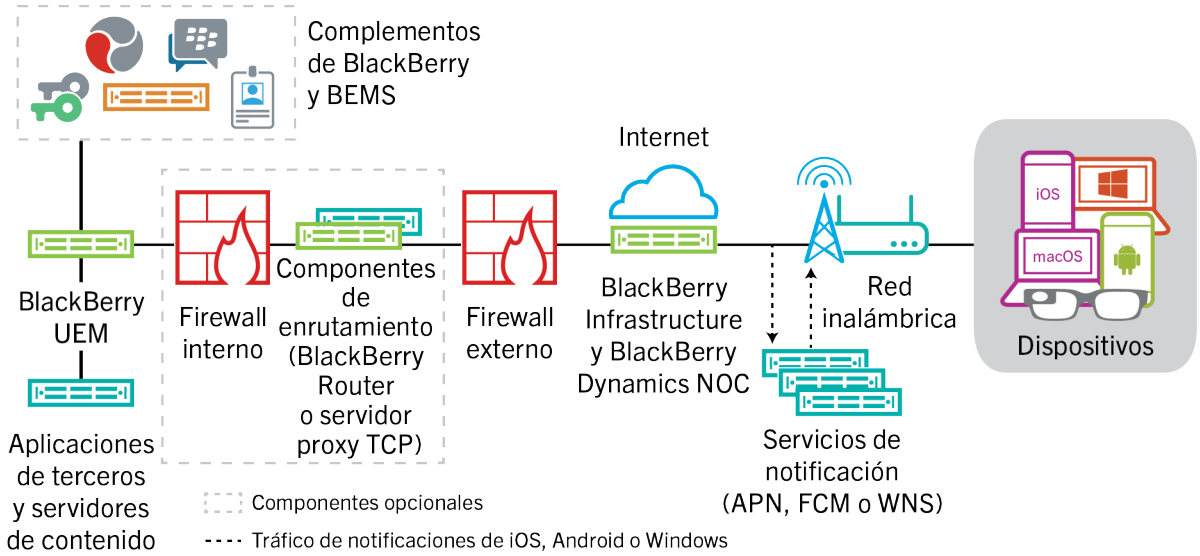
Gestión de aplicaciones

Función	iOS	macOS	Android	Windows 10
Distribución de las aplicaciones públicas de la tienda (App Store, Google Play, Windows Store, BlackBerry World)	√		√	√
Gestión del catálogo de aplicaciones de trabajo	√		√	√
Catálogo de aplicaciones de trabajo de marca	√			
Restricción de aplicaciones	√		√	
Distribución de aplicaciones internas	√		√	√
Añadir accesos directos de aplicación a dispositivos	√	√	√	

Arquitectura de BlackBerry UEM

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 los usuarios.

Arquitectura: solución BlackBerry UEM

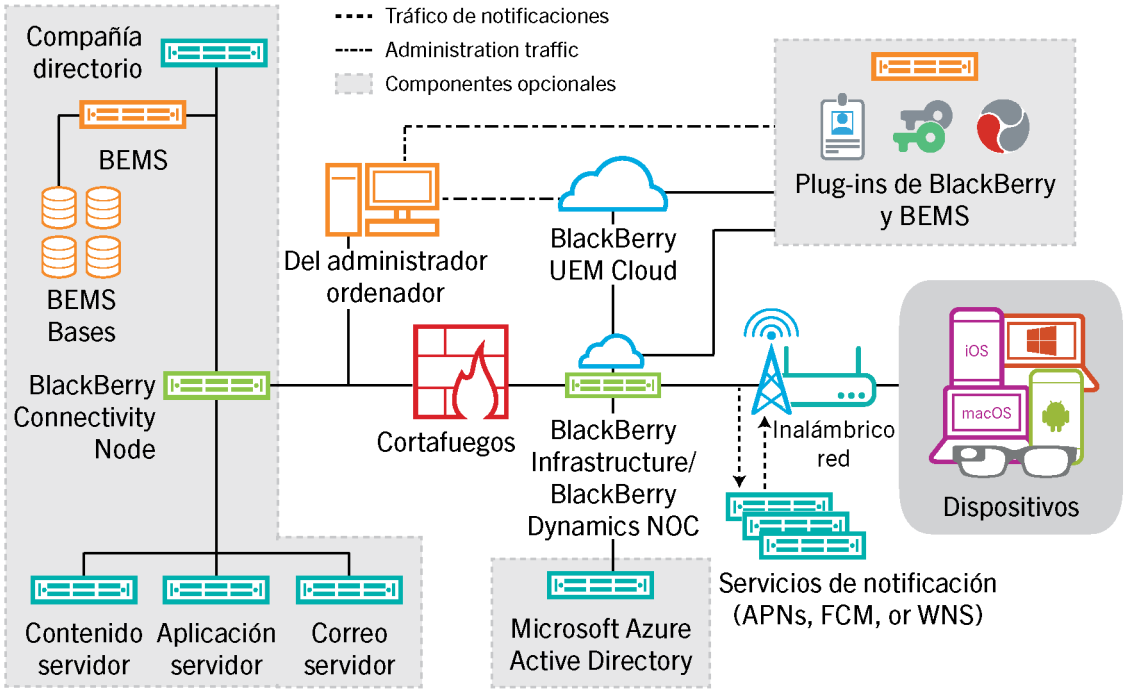


Componente	Descripción
BlackBerry UEM	BlackBerry UEM es una solución de gestión unificada de extremos que ofrece una gestión exhaustiva multiplataforma de dispositivos, aplicaciones y contenido con seguridad y conectividad integradas.
BlackBerry Infrastructure	BlackBerry Infrastructure es una red de 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. Se ha diseñado para administrar con eficiencia el transporte de datos entre los servicios BlackBerry y los dispositivos de los usuarios finales. Para empresas que utilizan UEM, BlackBerry Infrastructure registra la información del usuario para la activación de dispositivos, valida la información de licencias y proporciona una ruta de confianza entre la empresa y cada usuario basada en una autenticación mutua, sólida y cifrada. UEM mantiene una conexión constante con BlackBerry Infrastructure, lo que significa que las empresas requieren 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 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.

Componente	Descripción
BlackBerry Dynamics NOC	BlackBerry Dynamics NOC es un centro de operaciones de red que proporciona comunicaciones seguras entre las aplicaciones BlackBerry Dynamics en los dispositivos, UEM y BlackBerry Enterprise Mobility Server.
Dispositivos	BlackBerry UEM es compatible con los dispositivos iOS, macOS, Android y Windows.
Servicios de notificación	UEM envía notificaciones a los dispositivos para que se pongan en contacto con 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.
Componentes de enrutamiento	De forma predeterminada, 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. Si los estándares de seguridad de la empresa requieren 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 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	UEM funciona con productos empresariales adicionales de BlackBerry, como BlackBerry Enterprise Identity, BlackBerry 2FA y BlackBerry Workspaces, lo que le permite ampliar las capacidades de UEM en su empresa. Para obtener más información, consulte Productos y servicios complementarios. BlackBerry Enterprise Mobility Server proporciona servicios para enviar datos de trabajo hacia y desde las aplicaciones de BlackBerry Dynamics. Para obtener más información, consulte la documentación de BlackBerry Enterprise Mobility Server.

Arquitectura: solución BlackBerry UEM Cloud

La arquitectura de BlackBerry UEM Cloud se ha diseñado para ayudarle a administrar los dispositivos móviles de su empresa en un entorno de nube 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 los usuarios.



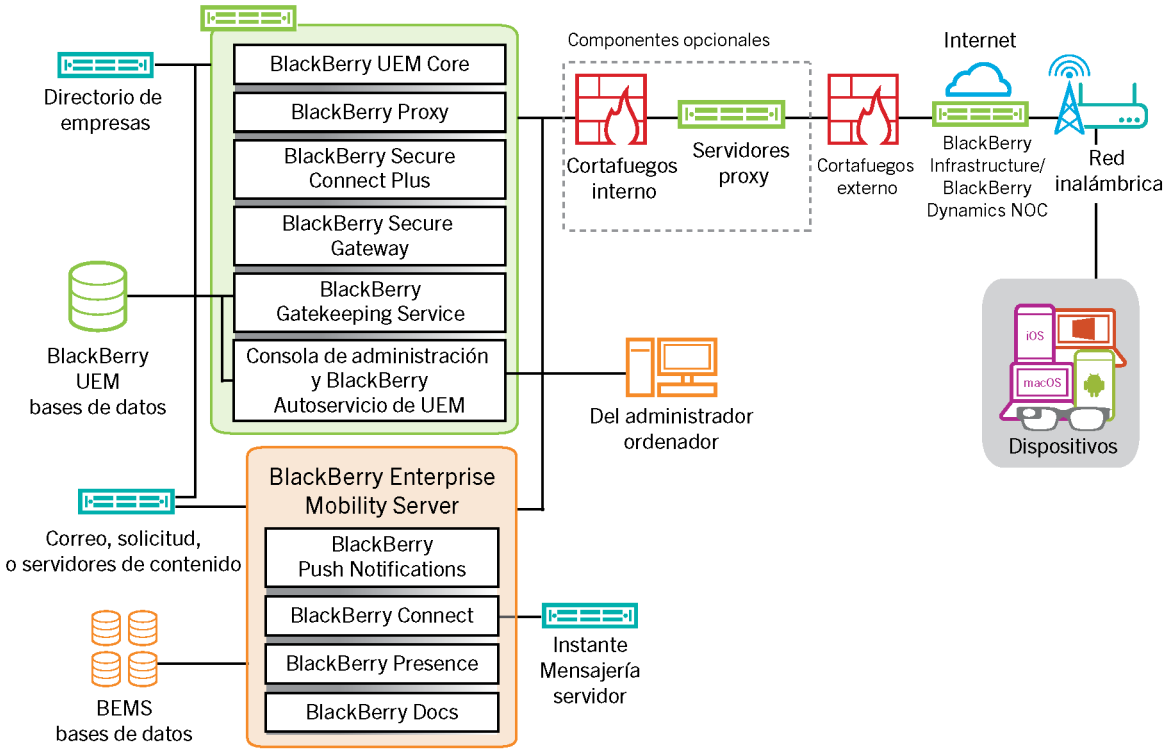
Componente	Descripción
BlackBerry UEM Cloud	BlackBerry UEM Cloud es un servicio que le permite administrar los dispositivos utilizados en el entorno de su empresa.
BlackBerry Infrastructure y BlackBerry Dynamics NOC	BlackBerry Infrastructure registra la información del usuario para la activación del dispositivo y valida la información de licencia. Al activar BlackBerry Secure Connect Plus o BlackBerry Secure Gateway, los datos en tránsito que utilizan estos servicios pasan a través de BlackBerry Infrastructure. BlackBerry Dynamics NOC es un NOC con ubicación independiente que ofrece comunicaciones seguras entre las aplicaciones de BlackBerry Dynamics en los dispositivos y el BlackBerry Proxy instalado detrás del firewall, como parte de BlackBerry Connectivity Node.
Dispositivos	BlackBerry UEM Cloud es compatible con los dispositivos iOS, macOS, Android y Windows.

Componente	Descripción
Servicios de notificación	UEM Cloud envía notificaciones a los dispositivos para que se pongan en contacto con 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 a los dispositivos 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. • WNS es un servicio que proporciona Microsoft para enviar notificaciones a los dispositivos Windows 10.
BlackBerry Connectivity Node	BlackBerry Connectivity Node es un componente opcional que se puede instalar dentro del firewall de la empresa. Incluye los siguientes componentes que añaden funcionalidad a UEM Cloud: • BlackBerry Cloud Connector conecta UEM Cloud al directorio de la empresa detrás del firewall para permitir la sincronización de atributos básicos, la funcionalidad de búsqueda y los servicios de autenticación de usuarios. Si no instala BlackBerry Connectivity Node y el directorio de su empresa está detrás del firewall, debe crear cuentas de usuario locales en UEM Cloud en lugar de utilizar las cuentas de usuario del directorio de la empresa. BlackBerry Cloud Connector no es necesario para que UEM Cloud se conecte a Microsoft Entra ID. • BlackBerry Proxy mantiene una conexión segura entre su empresa y BlackBerry Dynamics NOC, permitiendo que las aplicaciones de BlackBerry Dynamics puedan comunicarse de forma segura con los recursos de su empresa detrás del firewall. También admite BlackBerry Dynamics Direct Connect, que permite que los datos de aplicaciones omitan BlackBerry Dynamics NOC. • BlackBerry Gatekeeping Service envía los comandos a Exchange ActiveSync para agregar dispositivos a una lista de dispositivos admitidos cuando los dispositivos están activados en UEM Cloud. 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 UEM. • 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 proporciona una conexión segura a través de BlackBerry Infrastructure y UEM Cloud al servidor de correo de su empresa para dispositivos iOS.
Directorio de la empresa	UEM Cloud admite la conectividad con Microsoft Active Directory o el directorio LDAP de la empresa detrás del firewall utilizando BlackBerry Connectivity Node.
Microsoft Entra ID (anteriormente Azure AD)	Microsoft Entra ID es un servicio de gestión de directorios basado en la nube. Si su empresa utiliza Entra ID, puede conectarse a él en lugar de (o de forma adicional a) un directorio de la empresa protegido por el firewall.

Componente	Descripción
Contenido, aplicación y servidores de correo	Cuando se activa BlackBerry Secure Connect Plus o si los usuarios tienen aplicaciones de BlackBerry Dynamics, los dispositivos pueden conectarse a los servidores de la empresa sin tener que abrir una conexión directa entre el servidor e Internet. Los datos de trabajo en tránsito entre los servidores y los dispositivos se envían a través de BlackBerry Secure Connect Plus y de BlackBerry Infrastructure. Los datos de la aplicación de BlackBerry Dynamics se envían a través de BlackBerry Proxy y de BlackBerry Dynamics NOC. BlackBerry Secure Gateway proporciona una conexión segura a través de BlackBerry Infrastructure y BlackBerry Connectivity Node entre el servidor de correo de su empresa y los dispositivos iOS.
Complementos de BlackBerry y BEMS	UEM funciona con productos empresariales adicionales de BlackBerry, como BlackBerry Enterprise Identity, BlackBerry 2FA y BlackBerry Workspaces, lo que le permite ampliar las capacidades de UEM en su empresa. Para obtener más información, consulte Productos y servicios complementarios. BlackBerry Enterprise Mobility Server proporciona servicios para enviar datos de trabajo hacia y desde las aplicaciones de BlackBerry Dynamics. Para obtener más información, consulte la documentación de BlackBerry Enterprise Mobility Server.

Componentes BlackBerry UEM locales

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.



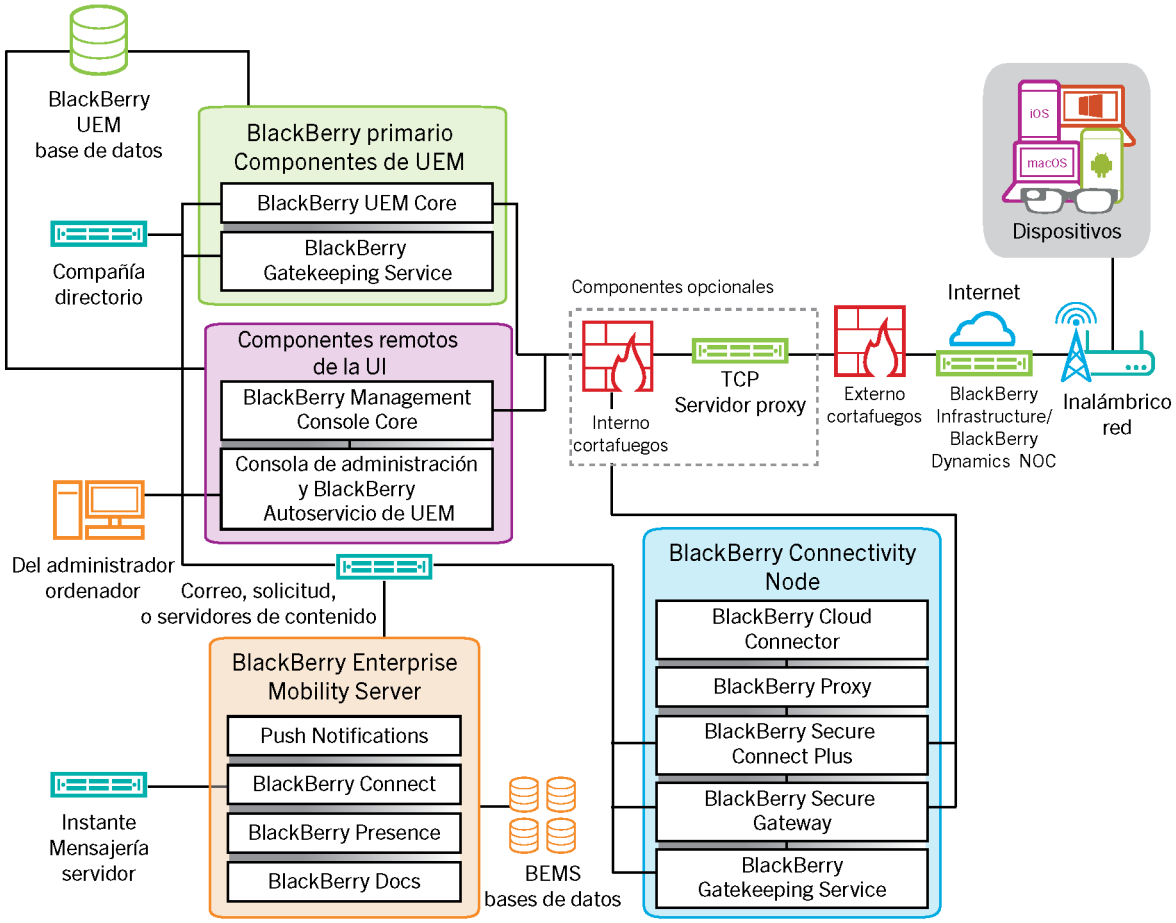
Nombre del componente	Descripción
BlackBerry UEM Core	BlackBerry UEM Core es el componente central de la arquitectura de UEM. Está constituido por varios subcomponentes que se encargan de: • Registro, supervisión, presentación de informes y funciones de administración • Los servicios de autenticación y autorización • Programación y envío de comandos, políticas de TI y perfiles a los dispositivos • Envío de datos de usuarios, políticas y otros datos de configuración a las aplicaciones BlackBerry Dynamics.
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.

Nombre del componente	Descripción
BlackBerry Secure Gateway	BlackBerry Secure Gateway proporciona una conexión segura a través de BlackBerry Infrastructure y 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 UEM. Desde la consola de administración, un administrador puede revisar, verificar y bloquear o permitir los dispositivos no administrados que intentan conectarse a un servidor de correo de la empresa.
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 UEM. Puede usar esta consola para gestionar la configuración del sistema, los usuarios, los dispositivos y las aplicaciones. Los usuarios pueden usar 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.
Base de datos de BlackBerry UEM	La base de datos de UEM es una base de datos relacional que contiene información de la cuenta de usuario y la información de configuración que UEM utiliza para administrar dispositivos y aplicaciones de BlackBerry Dynamics.
BlackBerry Enterprise Mobility Server	BEMS consolida varios servicios utilizados para enviar datos de trabajo hacia y desde las aplicaciones BlackBerry Dynamics, incluyendo lo siguiente: • 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: proporciona de forma segura mensajería instantánea, búsqueda en directorios de la empresa e información de presencia de usuarios a dispositivos iOS y Android. • BlackBerry Presence: proporciona estado de presencia en tiempo real a aplicaciones BlackBerry Dynamics. • 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, de reconfigurar el firewall ni de almacenes de datos duplicados. Las bases de datos de BEMS guardan la información de los usuarios, aplicaciones, políticas y configuraciones.
Servidores proxy o BlackBerry Router	De forma predeterminada, UEM establece una conexión directa con BlackBerry Infrastructure a través de los puertos 3101 y 443. Si los estándares de seguridad de la empresa requieren 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. UEM Core y BlackBerry Proxy son compatibles con el uso de un servidor proxy HTTP de terceros para conectarse a BlackBerry Dynamics NOC.

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 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 UEM Core, BlackBerry Proxy y BEMS.

Instalación distribuida local 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 UEM.



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

Nombre del componente	Descripción
Base de datos de BlackBerry UEM	La base de datos de UEM es una base de datos relacional que contiene información de la cuenta de usuario y la información de configuración que 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 UEM. Los dispositivos no administrados que intentan conectarse a un servidor de correo de la empresa se pueden revisar, verificar, bloquear o admitir a través de la consola de administración.
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 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 UEM Self-Service. Esto garantiza que estas interfaces respondan incluso cuando la carga en UEM Core es alta.
Consola de gestión y BlackBerry UEM Self-Service	La consola de gestión y UEM Self-Service proporcionan una interfaz de usuario basada en web para que el usuario y el administrador accedan a UEM. Se puede instalar por separado desde otros componentes. Puede usar esta consola para gestionar la configuración del sistema, los usuarios, los dispositivos y las aplicaciones. Los usuarios pueden acceder a UEM Self-Servicepara 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 UEM en el dominio de su empresa en un servidor diferente de UEM Core. Cada BlackBerry Connectivity Node contiene los componentes siguientes: • BlackBerry Cloud Connector: permite que los componentes de BlackBerry Connectivity Node se comuniquen con UEM Core. Toda la comunicación entre BlackBerry Cloud Connector y UEM Core se realiza a través de BlackBerry Infrastructure. • 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: 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: proporciona una conexión segura a través de BlackBerry Infrastructure y UEM con el servidor de correo de su empresa para dispositivos iOS. • BlackBerry Gatekeeping Service: administra la gestión del enlace para su servidor de correo. Si desea que BlackBerry Gatekeeping Service, que se ha instalado con los componentes principales de 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 BlackBerry Dynamics, incluyendo lo siguiente: • 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: proporciona de forma segura mensajería instantánea, búsqueda en directorios de la empresa e información de presencia de usuarios a dispositivos iOS y Android. • BlackBerry Presence: proporciona estado de presencia en tiempo real a aplicaciones BlackBerry Dynamics. • 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, de reconfigurar el firewall ni de almacenes de datos duplicados. 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 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 UEM Core, BlackBerry Proxy y BEMS.

Productos y servicios complementarios

En esta sección se proporciona información sobre los numerosos productos y servicios complementarios que se pueden utilizar con BlackBerry UEM.

Aplicaciones empresariales y BlackBerry Dynamics

Aplicaciones empresariales BlackBerry

BlackBerry ofrece varias aplicaciones empresariales que los administradores pueden cargar en los dispositivos o que los usuarios pueden instalar para ayudarles a acceder a datos de trabajo y ser más productivos.

Componente	Descripción
BlackBerry UEM Client	BlackBerry UEM Client permite que UEM gestione dispositivos iOS y Android. Los usuarios deben instalar UEM Client para activar dispositivos iOS o Android para la administración de dispositivos móviles con UEM. Los usuarios pueden descargar la versión más reciente de UEM Client desde App Store o Google Play. Una vez que los usuarios activen sus dispositivos, UEM Client permitirá a los usuarios realizar lo siguiente: • Comprobar si los dispositivos son compatibles con los estándares de la empresa • Ver los perfiles que se les han asignado • Ver las reglas de políticas de TI que se les han asignado • Acceder a las aplicaciones de trabajo • Creación de claves de acceso para aplicaciones BlackBerry Dynamics • Autenticación previa con BlackBerry 2FA • Acceder a un código OTP de software • Recuperar y enviar por correo electrónico archivos de registro de dispositivos • Desactivar sus dispositivos Para obtener más información, consulte la documentación de UEM Client.
BBM Enterprise	BBM Enterprise añade una capa de cifrado integral para mensajes de BBM enviados entre los usuarios de BBM Enterprise en su empresa y otros usuarios de BBM dentro y fuera de la empresa. BBM Enterprise está disponible para dispositivos con iOS, Android, Windows y macOS. BBM Enterprise utiliza una biblioteca cifrada validada por FIPS 140-2. Las claves de cifrado son propiedad de su empresa y nadie más puede acceder a ellas, ni siquiera BlackBerry. Para la mayoría de dispositivos, puede utilizar UEM para asignar BBM Enterprise a los usuarios. Al permitir que los usuarios puedan utilizar BBM Enterprise, podrán descargar la aplicación desde la tienda de aplicaciones adecuada. Para obtener más información, consulte la documentación de BBM Enterprise.

Aplicaciones de BlackBerry Dynamics

Las aplicaciones de productividad de BlackBerry Dynamics proporcionan a los usuarios acceso a los datos de trabajo y herramientas de productividad.

Aplicación	Descripción
BlackBerry Work	La aplicación BlackBerry Work proporciona un acceso seguro al correo de trabajo y permite a los usuarios ver y enviar archivos adjuntos, crear notificaciones de contacto personalizadas y administrar sus mensajes. Para obtener más información, consulte la documentación de BlackBerry Work.
BlackBerry Access	BlackBerry Access es un navegador seguro que permite a los usuarios tener acceso a las aplicaciones web e intranets del trabajo. BlackBerry Access también le permite habilitar el acceso a los recursos del trabajo o crear e implementar aplicaciones HTML5 complejas, mientras se mantiene un alto nivel de seguridad y cumplimiento. Para obtener más información, consulte la documentación de BlackBerry Access.
BlackBerry Connect	BlackBerry Connect permite la comunicación y la colaboración con la mensajería instantánea segura, la búsqueda de directorios de la empresa y la presencia de usuarios en una interfaz fácil de usar en el dispositivo del usuario. Para obtener más información, consulte la documentación de BlackBerry Connect.
BlackBerry Tasks	BlackBerry Tasks permite a los usuarios crear, editar y gestionar tareas que se sincronizan con Microsoft Exchange. Para obtener más información, consulte la documentación de BlackBerry Tasks.
BlackBerry Notes	BlackBerry Notes permite a los usuarios crear, editar y gestionar notas que se sincronizan con Microsoft Exchange en el dispositivo móvil que elijan. Para obtener más información, consulte la documentación de BlackBerry Notes.
BlackBerry BRIDGE	BlackBerry BRIDGE es una aplicación de Microsoft Intune activada para BlackBerry Dynamics. Le permite ver, editar y guardar documentos de forma segura utilizando aplicaciones de Microsoft gestionadas por Intune, como Microsoft Word, Microsoft PowerPoint y Microsoft Excel en BlackBerry Dynamics en dispositivos iOS y Android. Para obtener más información, consulte la documentación de BlackBerry Bridge.

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

Su organización también puede desarrollar aplicaciones BlackBerry Dynamics personalizadas mediante BlackBerry Dynamics SDK. Para obtener más información, consulte la documentación de BlackBerry Dynamics SDK.

Ventajas de BlackBerry Enterprise Identity

BlackBerry Enterprise Identity facilita a los usuarios el acceso a aplicaciones en la nube desde cualquier dispositivo, incluidos iOS, Android, así como desde plataformas informáticas tradicionales. Esta capacidad está estrechamente integrada con BlackBerry UEM, y unifica las soluciones EMM líderes del sector con el derecho y el control de todos sus servicios en la nube.

BlackBerry Enterprise Identity ofrece inicio de sesión único (SSO) a los servicios en la nube, como Microsoft 365, Google Workspace, BlackBerry Workspaces y muchos otros. Con el inicio de sesión único, los usuarios no tienen que realizar varios inicios de sesión ni recordar varias contraseñas. Los administradores también pueden agregar servicios personalizados a Enterprise Identity para ofrecer a los usuarios acceso a las aplicaciones internas.

Los administradores pueden usar la consola de UEM para gestionar los usuarios y agregar y gestionar administradores adicionales. La integración con UEM facilita la administración de usuarios y la autorización para acceder a aplicaciones y servicios en la nube desde sus dispositivos. Los servicios en la nube y los archivos binarios de aplicaciones móviles pueden agruparse y posteriormente asignarse a usuarios y grupos.

Para obtener más información, consulte la documentación de BlackBerry Enterprise Identity.

Ventajas de BlackBerry 2FA

BlackBerry 2FA proporciona a sus usuarios autenticación en dos fases para acceder a los recursos de la empresa. Le permite utilizar los dispositivos iOS y Android como segundo factor de autenticación mediante una solicitud de confirmación sencilla cuando los usuarios intentan conectarse a los recursos de su empresa.

Para los usuarios que no disponen de un dispositivo móvil o tienen un dispositivo móvil que no tiene suficiente conectividad para admitir BlackBerry 2FA en tiempo real, puede emitir identificadores de contraseña de un solo uso (OTP) basados en estándares. El primer factor de autenticación es la contraseña de directorio del usuario y el segundo es un código dinámico que aparece en la pantalla del identificador.

Puede administrar BlackBerry 2FA desde la consola de gestión de UEM. BlackBerry 2FA también se integra con BlackBerry Enterprise Identity. Puede utilizar BlackBerry 2FA para proporcionar un segundo factor de autenticación para los recursos cuyo acceso gestiona con Enterprise Identity.

Para obtener más información, consulte los documentos de BlackBerry 2FA.

Ventajas de BlackBerry Workspaces

BlackBerry Workspaces es una plataforma empresarial de gestión de archivos que permite a los usuarios acceder de forma segura, sincronizar, editar y compartir archivos y carpetas en varios dispositivos. BlackBerry Workspaces limita el riesgo de pérdida y de robo de datos integrando una función de seguridad con gestión de derechos digitales en todos los archivos, con el fin de que los contenidos permanezcan seguros y bajo el control del usuario incluso después de descargarlos y compartirlos con otros usuarios. Con el almacenamiento de archivos seguro y la posibilidad de transferir datos al mismo tiempo que se mantiene el control, tanto los empleados como TI pueden sentirse seguros a la hora de compartir datos y en lo que respecta a la seguridad de los documentos.

Los usuarios pueden acceder a BlackBerry Workspaces utilizando un navegador web o aplicaciones en los equipos con Windows y macOS, así como en los dispositivos iOS y Android. El contenido se sincroniza en todos los dispositivos del usuario cuando está en línea, de forma que puede gestionar, ver, crear, editar y añadir notas a los archivos desde cualquier dispositivo. Puede utilizar el complemento Workspaces para BlackBerry UEM para integrar la administración de Workspaces en la consola de administración de UEM.

Si su empresa también implementa BlackBerry Enterprise Identity, puede utilizar Enterprise Identity para administrar las autorizaciones de los usuarios a Workspaces.

Para obtener más información, consulte la documentación de BlackBerry Workspaces.

Ventajas de BlackBerry UEM Notifications

BlackBerry UEM Notifications se sirve de la comunicación en red en caso de crisis de BlackBerry AtHoc para permitir que los administradores puedan enviar mensajes y notificaciones importantes a usuarios y grupos desde la consola de administración de UEM.

Ya que UEM Notifications permite a los administradores gestionar dispositivos y notificaciones en la consola de administración de UEM, no necesitarán gestionar ni cotejar la información de contacto de los usuarios en varios sistemas ni enfrentarse a problemas de acceso en sistemas externos. UEM Notifications accede a la información de contacto mediante la sincronización de Microsoft Active Directory. UEM Notifications también ofrece opciones de entrega flexibles, como llamadas de voz con síntesis de voz, SMS y correos electrónicos, para que los usuarios reciban las alertas mediante su canal preferido, lo que aumenta las probabilidades de acción y cumplimiento.

Los administradores pueden controlar y gestionar las notificaciones enviadas, incluidos estados detallados de los mensajes según el método de entrega. UEM Notifications utiliza servicios de entrega autorizados por FedRAMP y proporciona un informe completo de todos los mensajes enviados y sus estados.

BlackBerry UEM Notifications solo está disponible para su uso en BlackBerry UEM local.

Para obtener más información, consulte la documentación Notificaciones UEM.

SDK de empresa BlackBerry

BlackBerry ofrece varias opciones de SDK para ayudar a su empresa a personalizar y ampliar su solución de BlackBerry.

SDK	Descripción
BlackBerry Dynamics SDK	BlackBerry Dynamics SDK proporciona un potente conjunto de herramientas que permiten a los desarrolladores centrarse en crear aplicaciones de productividad útiles en lugar de aprender a protegerlas, implementarlas y gestionarlas. Los desarrolladores pueden utilizar BlackBerry Dynamics SDK para desarrollar aplicaciones para las principales plataformas que aprovechan servicios valiosos, como comunicaciones seguras, intercambio de datos entre aplicaciones, presencia, inserción, búsqueda de directorios, autenticación con inicio de sesión único y gestión de acceso e identidades. Para obtener más información, consulte la documentación de BlackBerry Dynamics SDK.

SDK	Descripción
BlackBerry Web Services	Los BlackBerry Web Services son una colección de servicios web SOAP y REST que los desarrolladores pueden utilizar para crear aplicaciones para gestionar el dominio de UEM de la empresa, las cuentas de usuario y todos los dispositivos compatibles. Puede utilizar BlackBerry Web Services para automatizar muchas de las tareas que los administradores llevan a cabo con frecuencia mediante la consola de administración. Por ejemplo, puede crear una aplicación que automatice el proceso de creación de cuentas de usuarios, que agregue usuarios a varios grupos y que administre dispositivos de usuarios. Para obtener más información, consulte el contenido de BlackBerry Web Services.
BlackBerry Workspaces Android SDK	Los desarrolladores pueden utilizar el SDK BlackBerry Workspaces Android para desarrollar aplicaciones que permitan a los usuarios trabajar con archivos protegidos por BlackBerry Workspaces. Para obtener más información, consulte la documentación de BlackBerry Workspaces Android SDK.

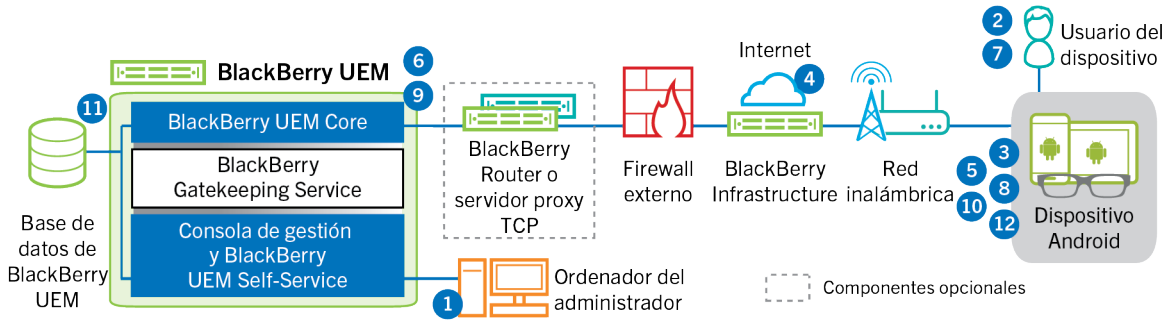
Para más información sobre cómo obtener y usar todas las herramientas para desarrolladores disponibles en BlackBerry, visite el sitio web de desarrolladores de BlackBerry.

Flujos de datos: activación de dispositivos y aplicaciones de BlackBerry Dynamics

Cuando un usuario activa un dispositivo con BlackBerry UEM, el dispositivo se asocia con 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 sobre los tipos de activación y cómo activar los dispositivos, consulte el contenido de Administración Activación de dispositivos.

Esta sección proporciona flujos de datos que detallan cómo se desplazan los datos a través del entorno de UEM de su organización cuando activa un dispositivo o una aplicación de BlackBerry Dynamics.

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



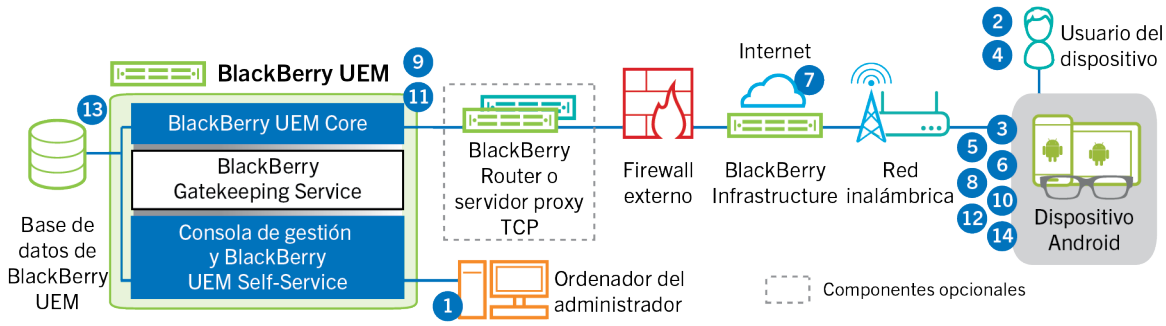
Este flujo de datos se aplica cuando permite que BlackBerry UEM gestione cuentas de Google Play.

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 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 con 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.

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

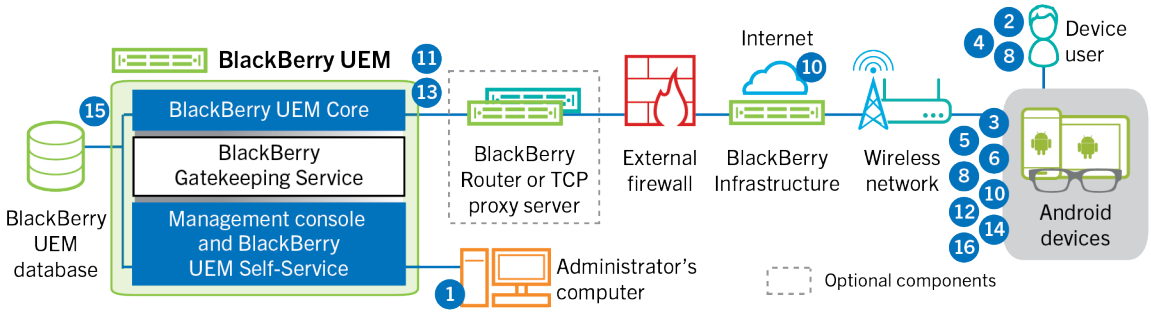
11. BlackBerry UEM realiza las siguientes acciones:

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 con 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.

1. Lleve a cabo las acciones siguientes:

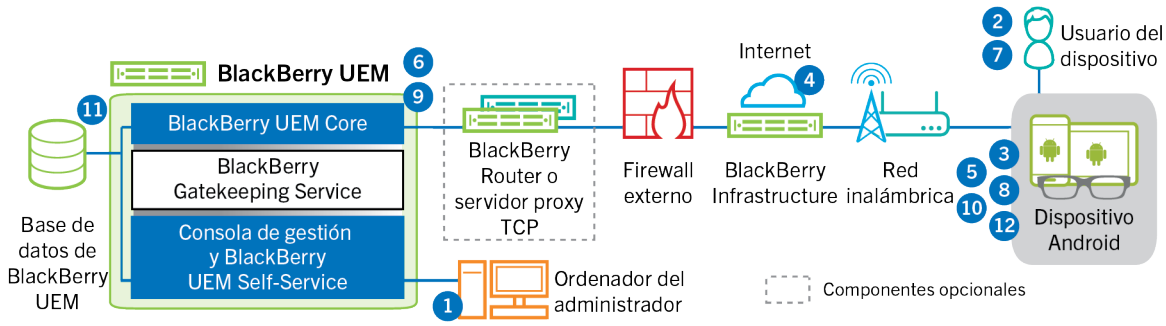
a. Agregue un usuario a BlackBerry UEM como una cuenta de usuario local o mediante la información de la cuenta recuperada desde el directorio de la empresa.
b. Asegúrese de que se ha asignado al usuario el tipo de activación "Solo espacio de trabajo".
c. Establezca la contraseña de activación del usuario.

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 sus credenciales 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 de 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 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 con Android Enterprise Trabajo y personal: privacidad de usuario en un dominio de Google



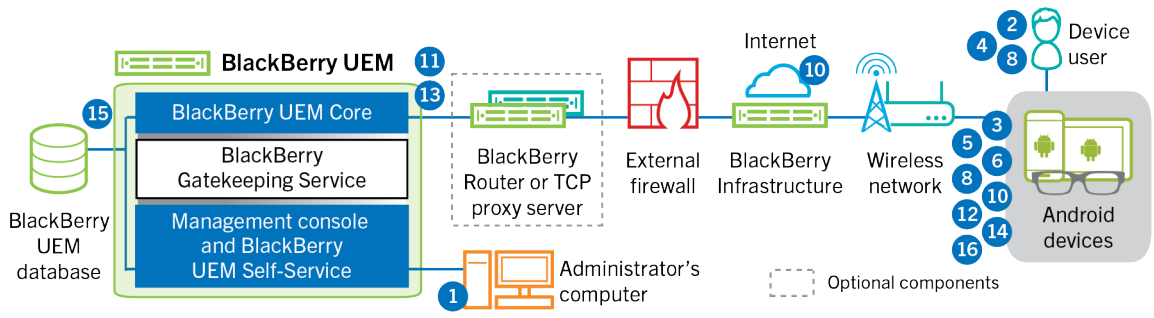
Este flujo de datos se aplica cuando BlackBerry UEM está conectado a un dominio de Google Cloud o Google Workspace.

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 gestionado 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 con 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 Google Workspace.

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. El dispositivo se comunica con el dominio de Google 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 de 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

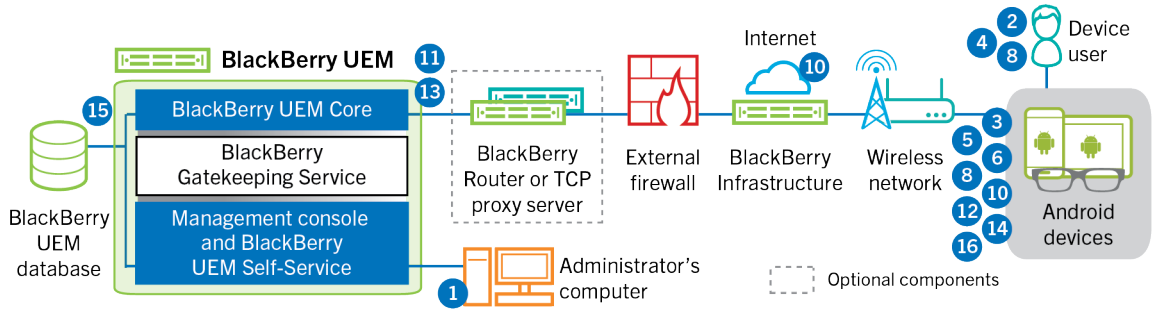
13. BlackBerry UEM realiza las siguientes acciones:

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 con 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 Google Workspace.

1. Lleve a cabo las acciones siguientes:

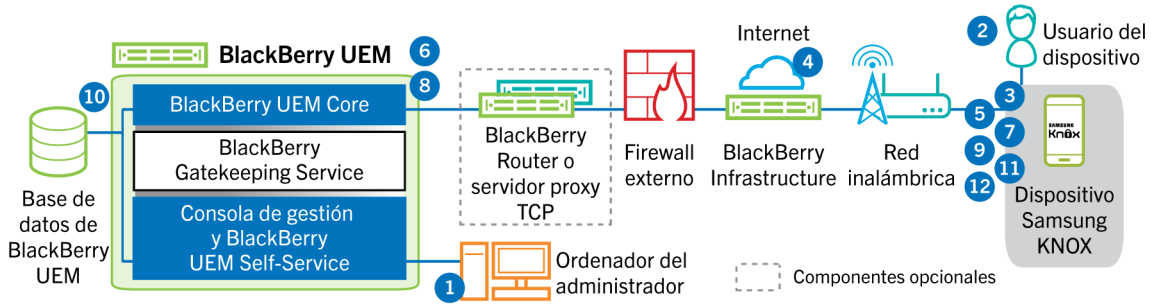
a. Compruebe que el usuario tiene una cuenta de Google que está asociada a la dirección de correo de trabajo del usuario. Opcionalmente, se puede configurar BlackBerry UEM para crear la cuenta de Google para el usuario durante el proceso de activación. Cuando BlackBerry UEM crea la cuenta de usuario 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. El dispositivo se comunica con el dominio de Google 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:

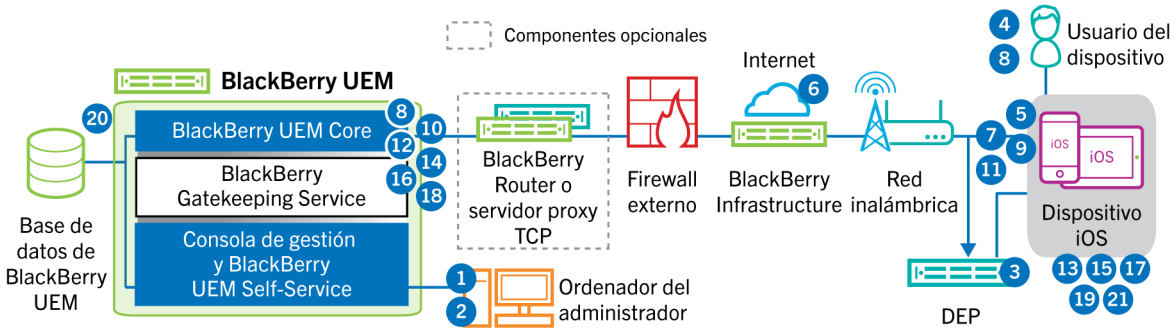
   a. Valida la solicitud del certificado de cliente con el ID de la sesión de inscripción en la sesión HTTP
   b. Firma la solicitud del certificado de cliente con el certificado raíz
   c. Envía el certificado de cliente firmado y el certificado raíz de nuevo a BlackBerry UEM Client

   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

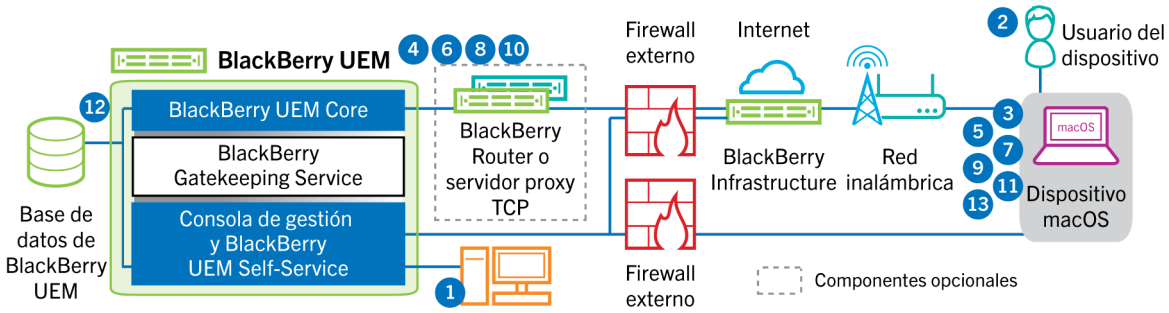
- Establezca una contraseña de activación del dispositivo y comunique el nombre de usuario y la contraseña al usuario directamente o por correo electrónico
- Anule la configuración de la contraseña de activación y comunique la dirección de BlackBerry UEM Self-Service al usuario para que pueda establecer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

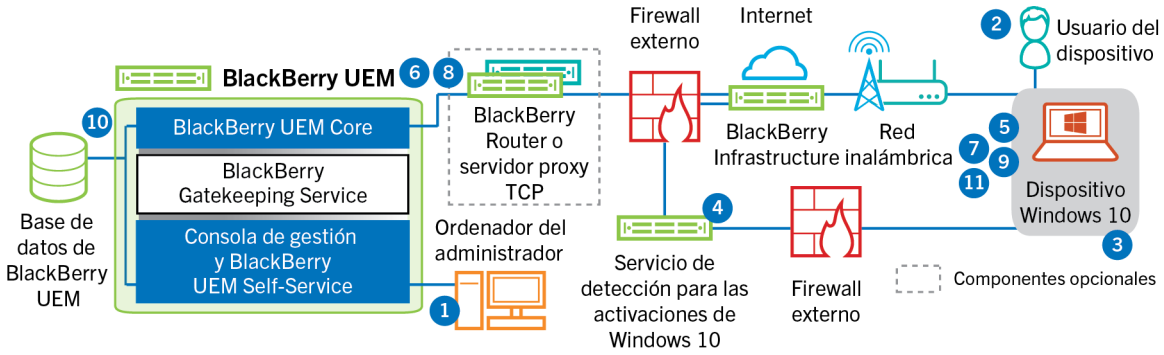
16. BlackBerry UEM envía el certificado de CA, la información de las capacidades de la CA y el certificado emitido por el dispositivo al MDM Daemon nativo.
17. El MDM Daemon nativo instala el perfil de MDM en el dispositivo. BlackBerry UEM Client notifica a BlackBerry UEM la correcta instalación del 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



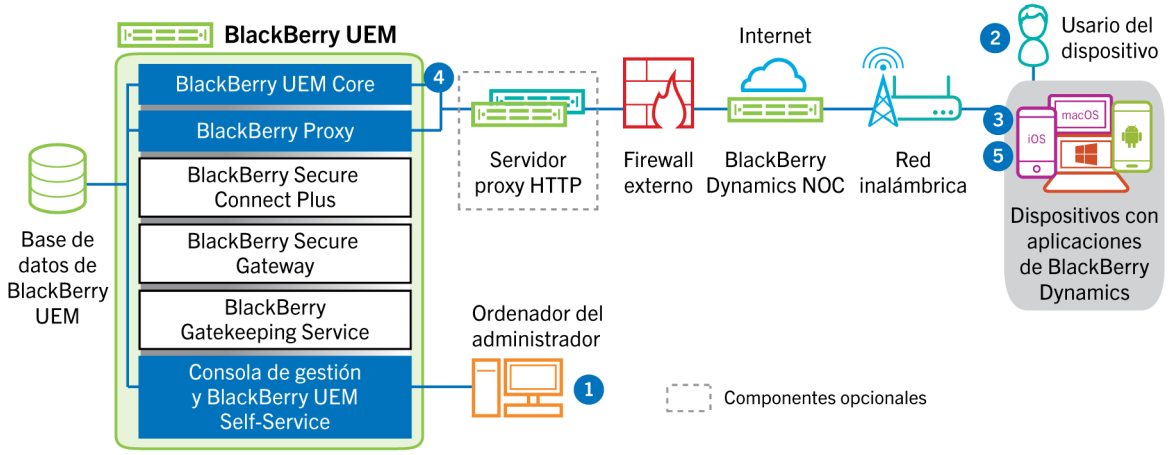
1. Lleve a cabo las acciones siguientes:
   a. Configurar el servicio de detección para simplificar las activaciones Windows 10
   b. Agregue un usuario a BlackBerry UEM como una cuenta de usuario local o mediante la información de la cuenta recuperada desde el directorio de la empresa.
   c. Utilice 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.



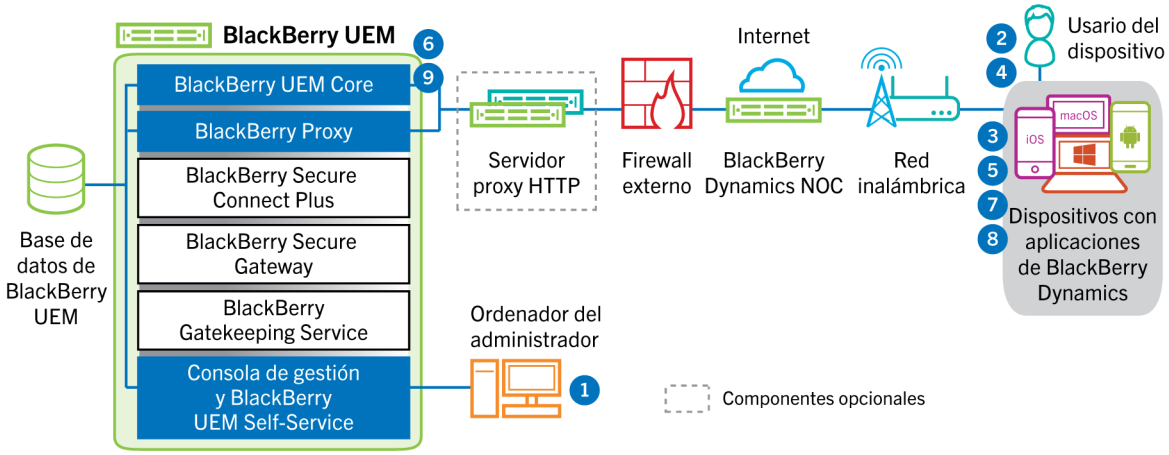
1. Un administrador realiza las siguientes acciones:
   a. Asigna una o más aplicaciones de BlackBerry Dynamics a un usuario.
   b. Emite las credenciales de activación (clave de acceso, contraseña de activación o código QR), o bien usa un proveedor de identidad de terceros, y las envía al usuario o 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.

Flujo de datos: 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.

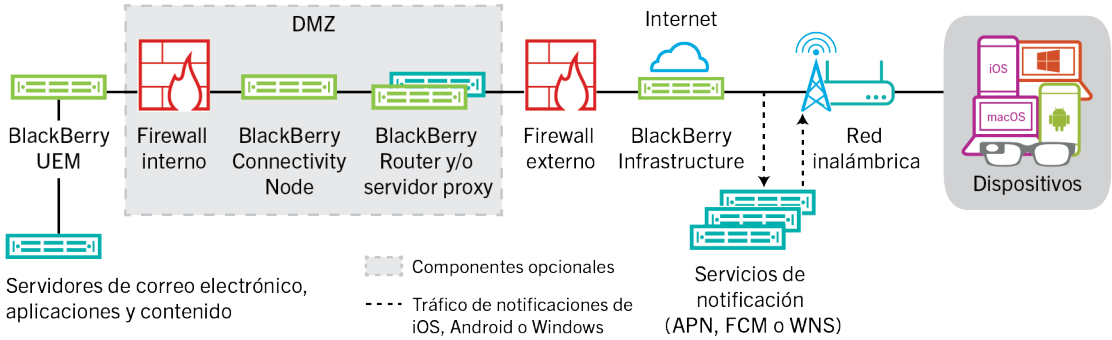
En esta sección se proporcionan flujos de datos que detallan cómo se desplazan los datos de trabajo a través del entorno de UEM de su organización.

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 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 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.
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 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 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 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.



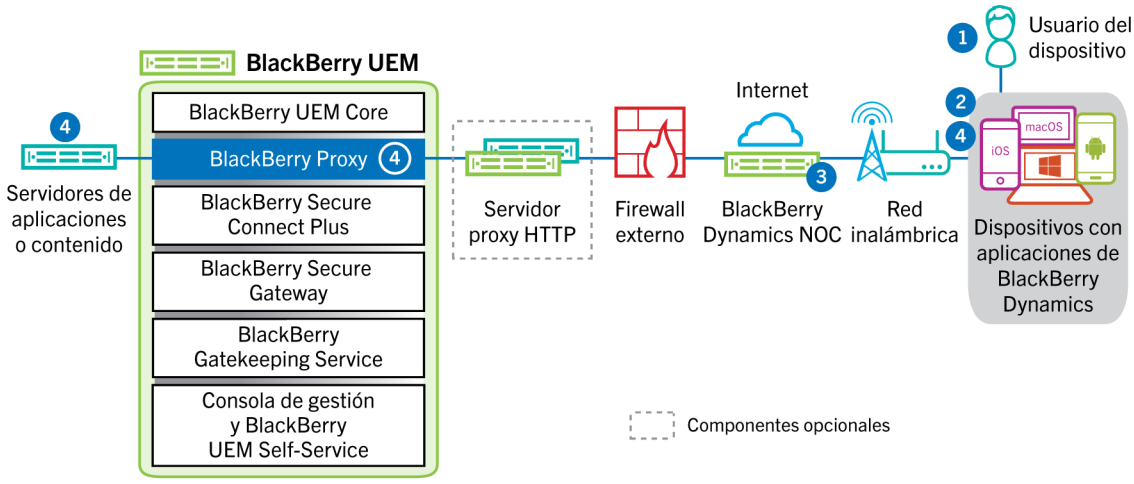
La tabla siguiente enumera las circunstancias en las que los dispositivos se conectan a BlackBerry UEM y a la red de su empresa a través de BlackBerry Infrastructure.

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 Flujos de datos: 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

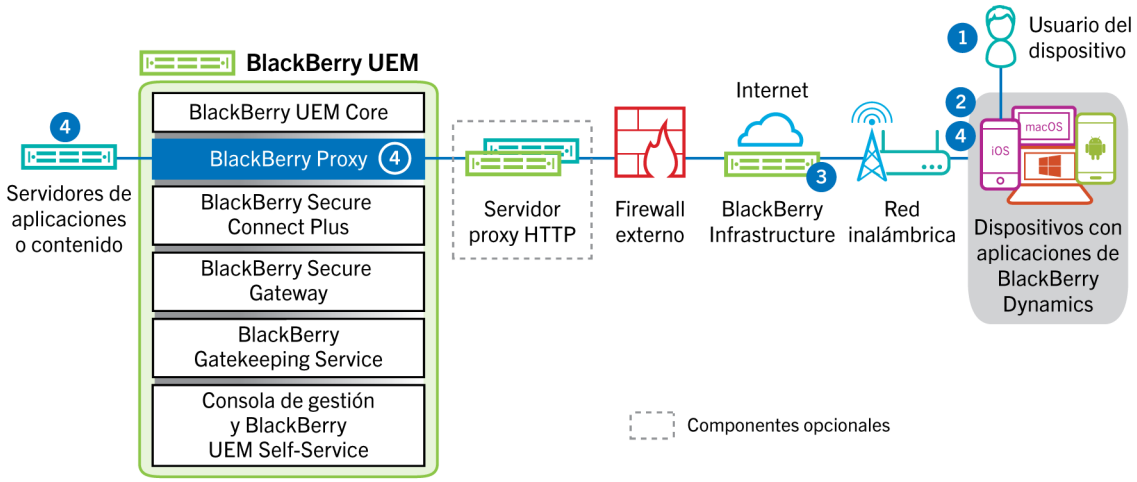
Proxy que transporta los datos de trabajo. Los datos de trabajo se cifran con una clave de sesión que BlackBerry Dynamics NOC no conoce.

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.

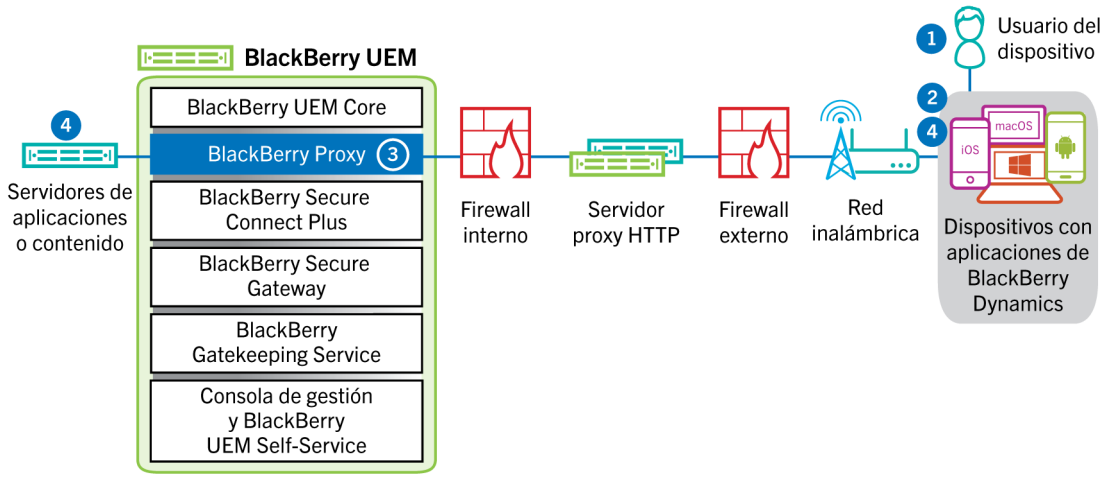
En este flujo de datos se describe cómo se desplazan los datos cuando una aplicación de BlackBerry Dynamics accede a un servidor de aplicaciones o de contenido en la empresa mediante BlackBerry Infrastructure BlackBerry UEM.



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.

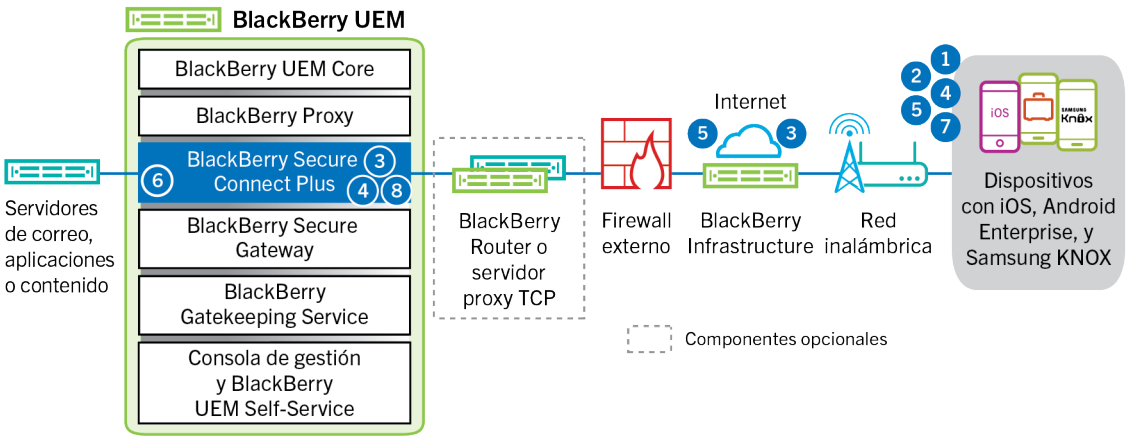


1. El usuario abre una aplicación de BlackBerry Dynamics para acceder a los datos de trabajo.
2. La aplicación de BlackBerry Dynamics establece una conexión TLS con BlackBerry Proxy.
3. BlackBerry Proxy se autentica con la aplicación de BlackBerry Dynamics. BlackBerry Proxy se autentica con la aplicación 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.

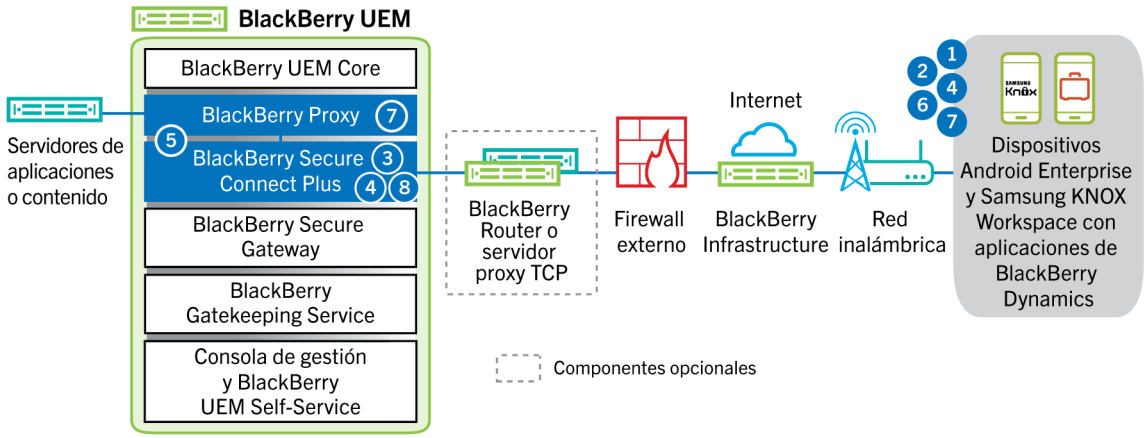
2. El dispositivo envía una solicitud a través de túnel TLS, a través del puerto 443, a BlackBerry Infrastructure para solicitar un túnel seguro a la red de trabajo. La señal se cifra de forma predeterminada con bibliotecas Certicom certificadas mediante FIPS-140. El túnel de señalización se somete a 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.

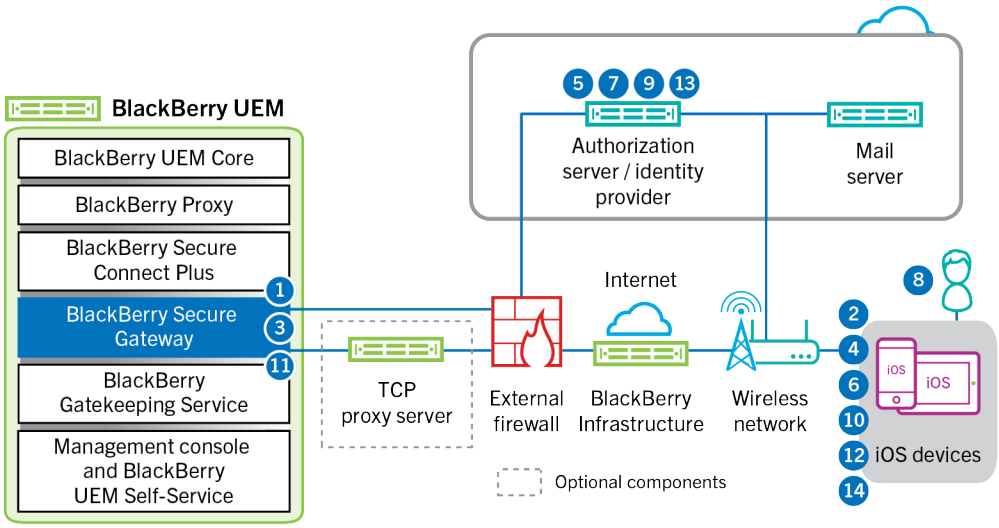
Si está utilizando BlackBerry Secure Connect Plus con aplicaciones de BlackBerry Dynamics en un dispositivo Android Enterprise o un dispositivo Samsung Knox Workspace, es recomendable que configure BlackBerry UEM para que no envíe los datos de las aplicaciones de BlackBerry Dynamics a través de BlackBerry 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 iOS se autentican con su servidor de correo a través de BlackBerry Secure Gateway mediante la autenticación moderna de Microsoft.



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

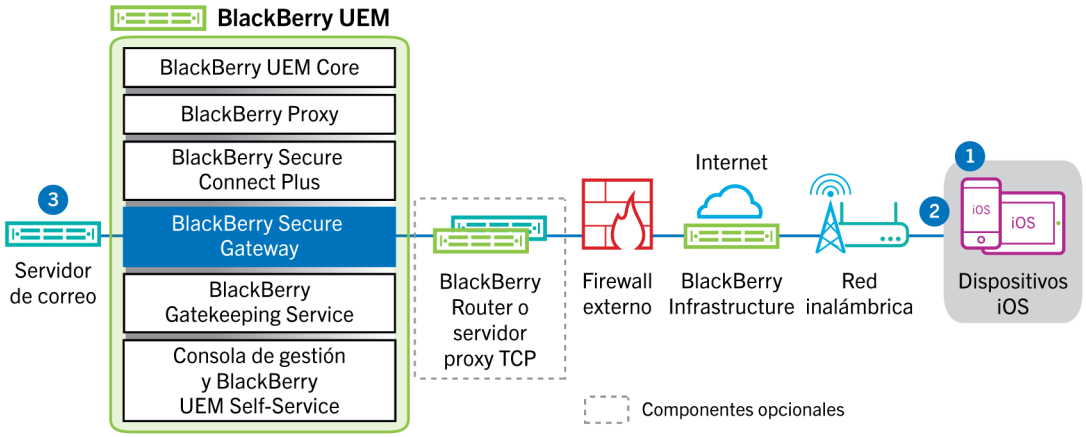
1. BlackBerry Secure Gateway recupera y almacena en caché los documentos de detección del servidor de autorización/proveedor de identidad especificados en los ajustes de configuración de BlackBerry Secure Gateway. BlackBerry Secure Gateway recupera tanto el documento de detección sin versión para dispositivos 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 Entra.
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

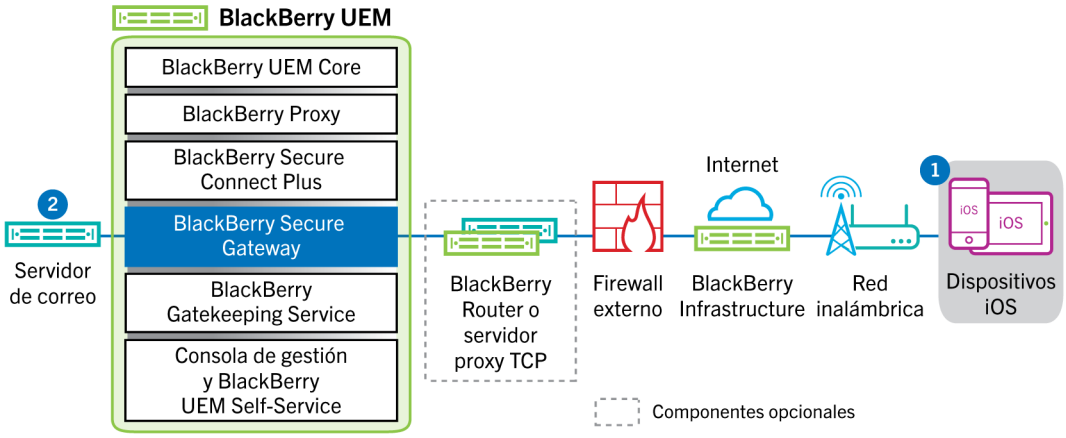
Este flujo de datos describe cómo se desplazan los datos del correo y del calendario de trabajo de dispositivos iOS al servidor de Exchange ActiveSync mediante BlackBerry Secure Gateway.



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.

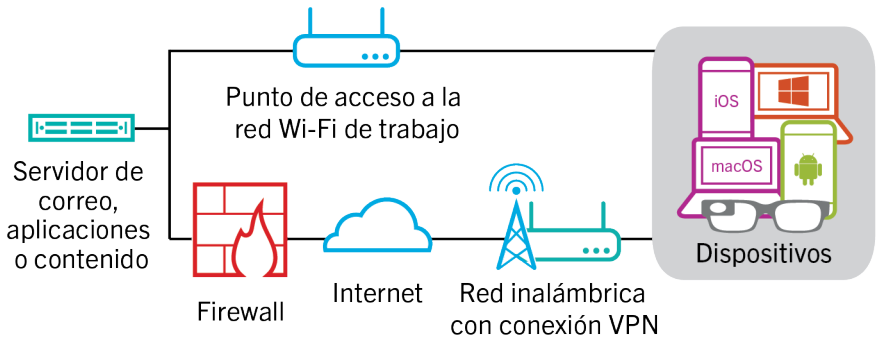


1. El cliente de correo electrónico nativo en iOS mantiene una conexión permanente con el servidor de correo a través de un canal cifrado y autenticado entre BlackBerry Infrastructure y BlackBerry Secure Gateway, y detecta los cambios en las carpetas configuradas para la sincronización en el servidor 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.

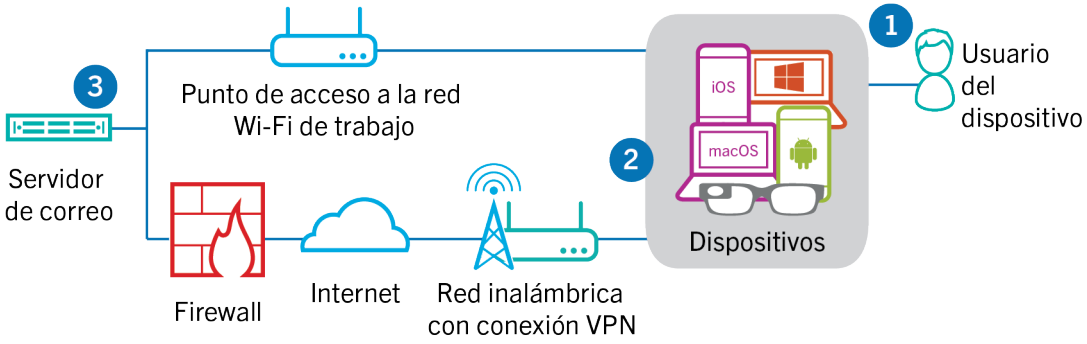


La siguiente tabla describe cuándo la red VPN de la empresa o la red Wi-Fi de trabajo utilizan dispositivos para conectarse a la red de su empresa.

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

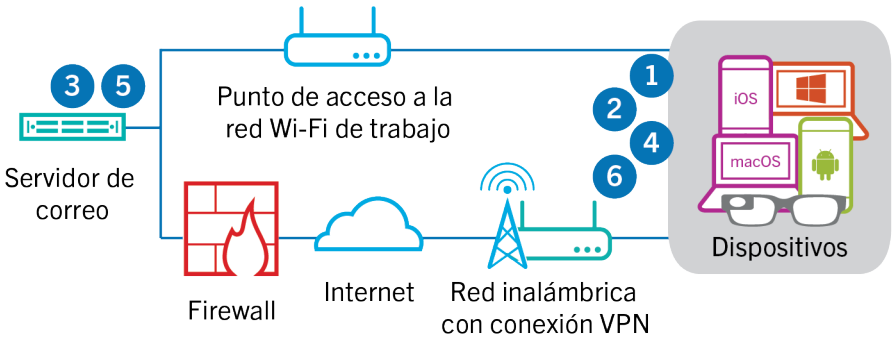
Este flujo de datos describe cómo se desplazan los datos del correo electrónico del trabajo y los datos del calendario desde el dispositivo al servidor de correo a través de la VPN o la red Wi-Fi de trabajo de la empresa mediante Exchange ActiveSync.



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

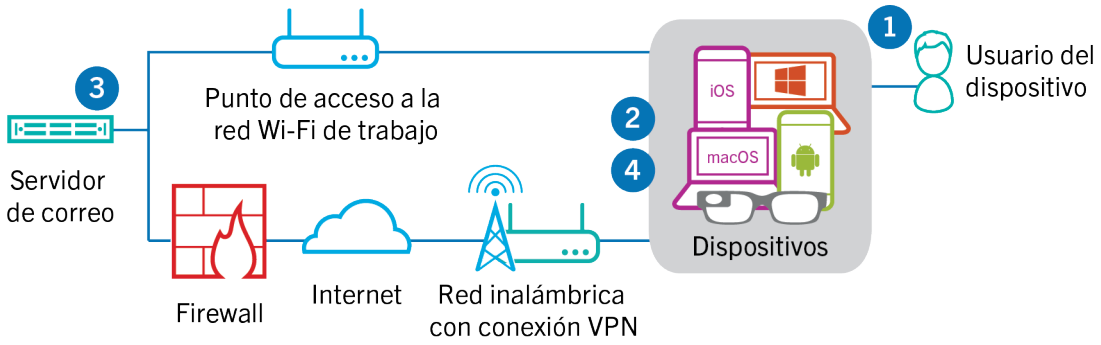
Este flujo de datos describe cómo se desplazan los datos del correo electrónico del trabajo y los datos del calendario desde el dispositivo al servidor de correo a través de la VPN o la red Wi-Fi de trabajo de la empresa mediante Exchange ActiveSync.



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.



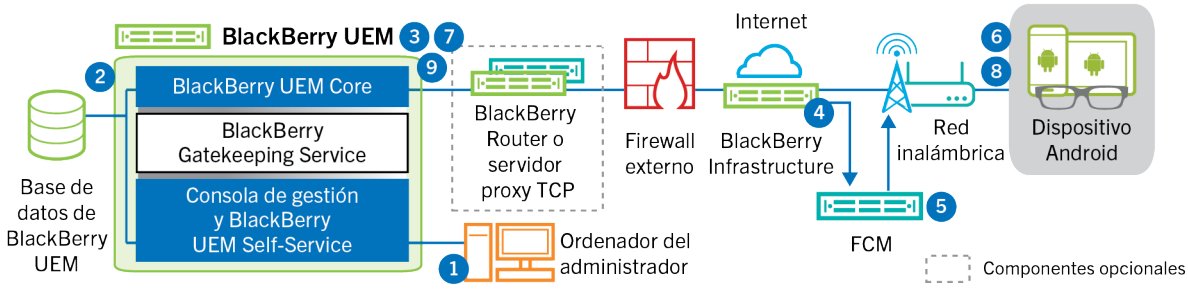
1. El usuario abre una aplicación de trabajo para ver los datos de trabajo. Por ejemplo, el usuario abre el navegador de trabajo para desplazarse por la intranet o utiliza una aplicación desarrollada de forma interna para acceder a los datos de los clientes de la empresa.
2. La aplicación establece una 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.

Flujos de datos: 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.

Esta sección proporciona flujos de datos que detallan cómo los se desplazan los datos a través del entorno de UEM de su organización cuando los dispositivos reciben actualizaciones de configuración.

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



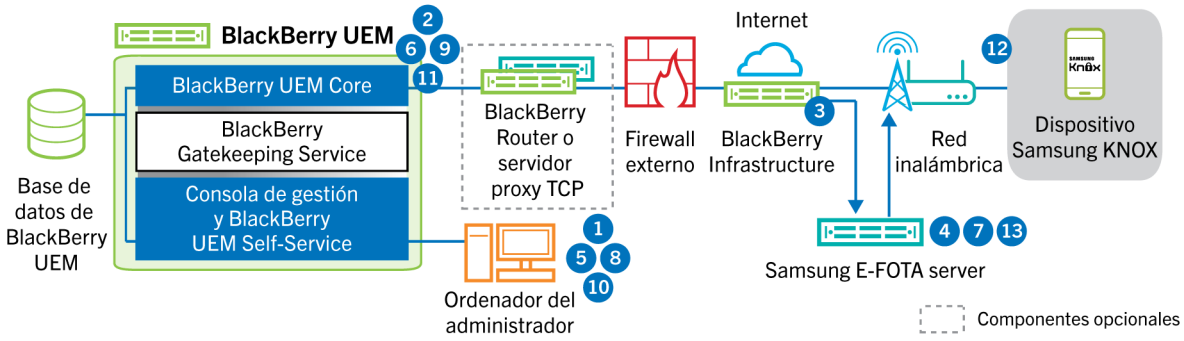
1. Se lleva a cabo una acción en la consola de administración que desencadena una actualización de la configuración de un dispositivo Android.
2. Las actualizaciones se aplican a BlackBerry UEM y se identifican los objetos que se deben compartir con el dispositivo.
3. BlackBerry UEM Core se pone en contacto 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 FCM 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.

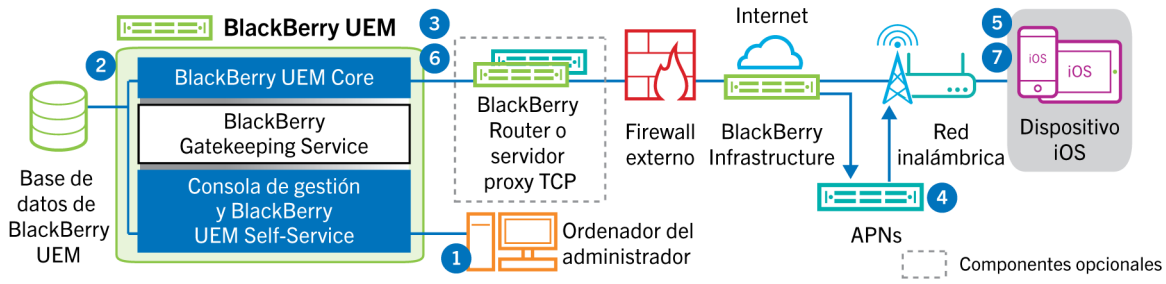
Flujo de datos: actualización del firmware en dispositivos Samsung Knox

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.



1. Un administrador puede agregar el ID de cliente y la clave de licencia de E-FOTA de 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 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 proveedor 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 E-FOTA verifica los criterios y devuelve la información de firmware 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.

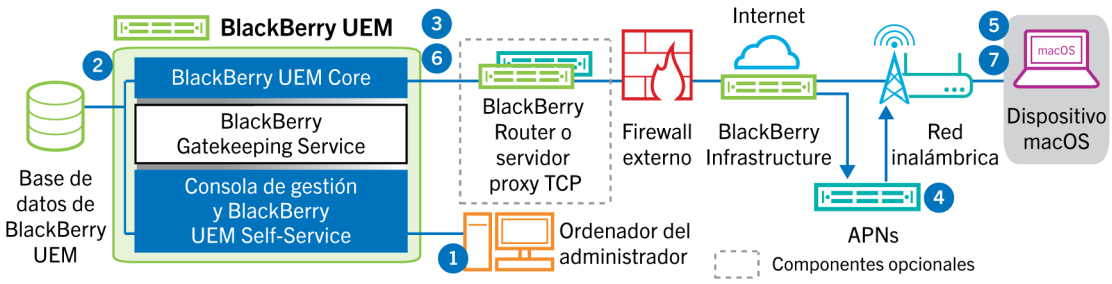
Flujo de datos: recepción de actualizaciones de configuración en un dispositivo iOS



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.

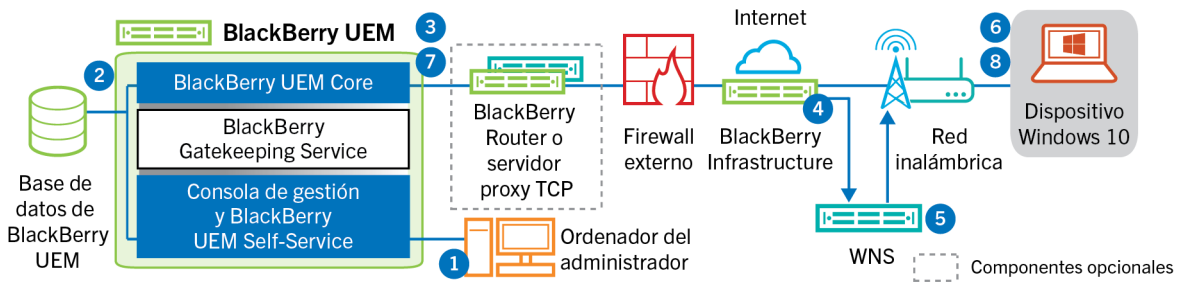
Flujo de datos: recepción de actualizaciones de configuración en un dispositivo macOS



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

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