BlackBerry UEM

Administración de dispositivos Android

Administración

12.16

Contents

Gestión de dispositivos Android

BlackBerry UEM le ofrece una administración precisa de la forma en que se conectan los dispositivos Android a su red, las capacidades activadas y las aplicaciones disponibles. Si los dispositivos son propiedad de su empresa o sus usuarios, puede ofrecer acceso móvil a la información de su organización a la vez que la protege de cualquier persona que debiera tener acceso.

Esta guía describe las opciones que tiene para administrar dispositivos Android y le ayuda a encontrar los detalles que necesita para sacar el máximo partido a todas las funciones disponibles.

Gestión de los dispositivos accesorios

Puede activar y gestionar los dispositivos accesorios con Android en BlackBerry UEM. Los dispositivos accesorios, como las gafas inteligentes, proporcionan a los usuarios acceso manos libres a información visual como notificaciones, instrucciones paso a paso, imágenes y vídeo y permiten a los usuarios emitir comandos de voz, escanear códigos de barras y utilizar la navegación GPS.

BlackBerry UEM es compatible con los siguientes dispositivos accesorios:

- Vuzix M300 Smart Glasses

Para gestionar los dispositivos accesorios, siga las instrucciones para dispositivos con Android. Las siguientes funciones de BlackBerry UEM son compatibles con los dispositivos accesorios:

- Activación del dispositivo mediante un QR Code
- Políticas de TI
- Wi-Fi, VPN, conectividad de empresa, conformidad y perfiles de certificado
- BlackBerry Secure Connect Service
- Comandos del dispositivo
- Administración de aplicaciones
- Grupos de dispositivos
- Servicios de ubicación

Los dispositivos accesorios utilizan el BlackBerry UEM Client para la activación. Puede activar los dispositivos accesorios mediante un código QR en lugar de una contraseña de activación.

Lo que puede controlar en los dispositivos Android

BlackBerry UEM le proporciona todas las herramientas que necesita para controlar las funciones que los dispositivos Android le permiten administrar. También incluye funciones que le permiten proporcionar un acceso seguro a los usuarios a recursos de trabajo sin administrar en su totalidad el dispositivo.

Nivel de control	Descripción
Dispositivos no administrados activaciones de Privacidad del usuario	Puede activar un dispositivo en BlackBerry UEM con el tipo de activación "Privacidad del usuario" para proporcionar un acceso seguro a los recursos de trabajo sin administrar el dispositivo. Esta opción suele utilizarse para dispositivos BYOD. Estas activaciones pueden permitir que el usuario acceda a su red a través de VPN mediante BlackBerry 2FA, compartir archivos de forma segura con BlackBerry Workspaces, e instalar aplicaciones BlackBerry Dynamics como BlackBerry Work y BlackBerry Access para acceder al correo de trabajo y a su intranet de trabajo.
Dispositivos administrados con un perfil de trabajo Activaciones de Trabajo y personal: privacidad de usuario (Android Enterprise)	Los dispositivos Android Enterprise se pueden administrar, pero es necesario permitir el uso personal mediante la creación de un perfil de trabajo en el dispositivo que separe los datos de trabajo de los datos personales. Esta opción mantiene la privacidad de datos personales del usuario en el perfil personal, pero le permite administrar los datos del trabajo utilizando los comandos y las reglas de la política de TI. Puede administrar las aplicaciones de trabajo de un dispositivo, incluidas las aplicaciones BlackBerry Dynamics. Puede borrar los datos del trabajo, pero no los datos personales, del dispositivo. Los datos personales y los datos de trabajo están protegidos mediante el cifrado y la autenticación de contraseña. Esta opción se utiliza con frecuencia dispositivos de propiedad corporativa, activación para uso personal (COPE) y BYOD.
Dispositivos administrados completamente con un perfil de trabajo Activaciones de Trabajo y personal: control total (Android Enterprise)	Los dispositivos Android Enterprise se pueden administrar por completo, pero es necesario permitir cierto uso personal mediante la creación de un perfil de trabajo en el dispositivo que separe los datos de trabajo de los personales, pero que permita que su empresa mantenga el control total sobre el dispositivo y borre todos los datos de este. Algunas reglas de políticas de TI pueden aplicarse por separado a los perfiles de trabajo y personales. Puede administrar las aplicaciones de trabajo de un dispositivo, incluidas las aplicaciones BlackBerry Dynamics. Puede registrar SMS, MMS y llamadas telefónicas que se hayan emitido y recibido en el dispositivo. Los datos personales y los datos de trabajo están protegidos mediante el cifrado y la autenticación de contraseña. Esta opción suele utilizarse para dispositivos COPE.

Nivel de control	Descripción
Dispositivos administrados completamente Activaciones de Solo espacio de trabajo (Android Enterprise)	Los dispositivos Android Enterprise se pueden administrar completamente y pueden tener un perfil de trabajo, pero no un perfil personal. Esta opción le permite administrar todo el dispositivo con comandos y reglas de políticas de TI. Puede administrar las aplicaciones de trabajo de un dispositivo, incluidas las aplicaciones BlackBerry Dynamics. Puede registrar SMS, MMS y llamadas telefónicas que se hayan emitido y recibido en el dispositivo. Todos los datos del dispositivo estarán protegidos mediante cifrado y un método de autenticación como una contraseña. Esta opción se utiliza con frecuencia dispositivos de propiedad corporativa y solo de uso laboral (COBO).
Administración del dispositivo activaciones de Controles de MDM	Puede administrar los dispositivos Android con versiones 9.x y anteriores mediante el uso de comandos y reglas de políticas de TI. No se crea un espacio de trabajo separado en el dispositivo y no hay seguridad adicional para los datos de trabajo. Para proporcionar seguridad a los datos del trabajo, puede instalar aplicaciones de BlackBerry Dynamics. Este tipo de activación está obsoleto para los dispositivos con Android 10. Para obtener más información, https://support.blackberry.com/community para leer el artículo 48386. Puede utilizar grupos de dispositivos y perfiles de conformidad para gestionar lo que pasa con los dispositivos activados con activaciones "Controles de MDM" que se actualicen a Android 10. Para obtener más información, consulte el contenido de Administración.

Android Enterprise proporciona una compatibilidad completa para administrar dispositivos Android, con la inclusión de las siguientes funciones:

- Aplicar los requisitos de la contraseña
- Controlar las capacidades del dispositivo mediante el uso de políticas de TI (por ejemplo, desactivar la cámara o Bluetooth)
- Ejecutar reglas de cumplimiento
- Crear perfiles de conexión Wi-Fi y VPN (con proxy)
- Sincronizar correo, contactos y calendarios con dispositivos
- Enviar certificados CA y de cliente a dispositivos para su autenticación y S/MIME
- Administrar las aplicaciones obligatorias, las públicas permitidas y las internas
- Localizar y proteger dispositivos perdidos o robados

Los dispositivos Android Enterprise que se activan con BlackBerry UEM también son compatibles con controles adicionales disponibles solamente para dispositivos Samsung Knox Platform for Enterprise y para dispositivos BlackBerry con tecnología de Android.

BlackBerry UEM también es compatible con dispositivos con activaciones de Samsung Knox Workspace, así como con Samsung Knox Platform for Enterprise; sin embargo, los tipos de activación de Samsung Knox caerán en desuso en una versión futura. Para obtener más información, visite https://support.blackberry.com/community para leer el artículo 54614.

Nota: Algunas funciones y aplicaciones de BlackBerry Dynamics no están disponibles con todos los niveles de licencia. Para obtener más información sobre las licencias disponibles, consulte el contenido referente a licencias.

Pasos para administrar dispositivos con Android

Paso	Acción
1	Instale y configure BlackBerry UEM de acuerdo con las instrucciones de instalación.
2	Si su organización tiene la intención de administrar dispositivos Android Enterprise, configure una cuenta administrada de Google Play o una conexión a su Google Cloud o dominio de G Suite.
3	Configure las políticas de TI para dispositivos. Asigne políticas de TI a grupos de usuarios o usuarios individuales.
4	Configure perfiles para dispositivos. Asigne perfiles a grupos de usuarios o usuarios individuales.
5	Especifique las aplicaciones que los dispositivos pueden o deben instalar.
6	Active los dispositivos.
7	Administre y controle los dispositivos.

Compatibilidad con las activaciones de Android Enterprise

El modo en que los usuarios activan los dispositivos Android Enterprise puede depender de diversos factores, como la versión del sistema operativo Android, el control que su empresa desea tener sobre los dispositivos de los usuarios y el modo en que su empresa utiliza los servicios de Google. Su empresa puede interactuar con los servicios de Google de las siguientes formas:

Conexión con los servicios de Google	Descripción
Cuentas de Google Play gestionadas	BlackBerry UEM no está conectado a un dominio de Google. Puede utilizar cuentas de Google Play gestionadas para permitir a los usuarios descargar e instalar aplicaciones de trabajo mediante Google Play. Para obtener más información, consulte Compatibilidad con las activaciones de Android Enterprise mediante cuentas de Google Play gestionadas
Dominio de G Suite	Su empresa cuenta con un dominio de G Suite, compatible con todos los servicios de G Suite, como Gmail, Google Calendar y Google Drive. Para obtener más información, consulte Compatibilidad de las activaciones Android Enterprise con un dominio de G Suite
Dominio de Google Cloud	Su empresa dispone de un dominio de Google Cloud, que proporciona cuentas de Google gestionadas a los usuarios. Su empresa no usa servicios de G Suite, como Gmail, Google Calendar y Google Drive para el correo, el calendario y la administración de datos de su empresa. Para obtener más información, consulte Compatibilidad de las activaciones Android Enterprise con un dominio de Google Cloud
Sin servicios de Google	Las políticas de seguridad de la empresa no le permiten utilizar los servicios de Google. Para obtener más información, consulte Compatibilidad de dispositivos Android Enterprise sin acceso a Google Play

Para obtener más información sobre cómo configurar BlackBerry UEM para conectarse a un dominio de Google o utilizar cuentas de Google Play gestionadas, consulte el contenido de Configuración local o el contenido de Configuración en la nube.

Compatibilidad con las activaciones de Android Enterprise mediante cuentas de Google Play gestionadas

Si su empresa no tiene un dominio de Google o no desea conectar BlackBerry UEM a su dominio de Google, puede activar los dispositivos Android Enterprise para utilizar cuentas de Google Play gestionadas. Las cuentas de Google Play gestionadas le permiten agregar aplicaciones internas a Google Play que solo se podrán descargar desde los dispositivos de usuarios activados. Para obtener más información acerca de las cuentas de Google Play gestionadas, consulte https://support.google.com/googleplay/work/.

Para utilizar cuentas de Google Play gestionadas con BlackBerry UEM, utilice cualquier cuenta de Google o Gmail para conectar BlackBerry UEM a Google. No se enviará ninguna información de identificación personal acerca de los usuarios a Google tras conectar BlackBerry UEM a Google. Además, puede permitir que los usuarios activen dispositivos Android Enterprise y descarguen aplicaciones de trabajo mediante Google Play. Para obtener más información acerca de cómo configurar BlackBerry UEM para permitir su uso con dispositivos Android Enterprise, consulte el contenido de Configuración local o el contenido de Configuración de UEM Cloud.

Compatibilidad de las activaciones Android Enterprise con un dominio de G Suite

Si ha configurado BlackBerry UEM para conectarse a un dominio de G Suite, debe realizar las siguientes tareas antes de que los usuarios puedan activar los dispositivos Android Enterprise.

Antes de empezar: Configure BlackBerry UEM para que sea compatible con dispositivos Android Enterprise. Para obtener más información sobre la configuración de BlackBerry UEM para ser compatible con dispositivos Android Enterprise, consulte el contenido de Configuración local o el contenido de Configuración de UEM Cloud.

1. En el dominio de G Suite, cree cuentas de usuario para los usuarios de Android.
2. Seleccione la opción **Aplicar política de EMM** en el dominio de G Suite.

   Esta configuración es necesaria para dispositivos con el tipo de activación Solo espacio de trabajo y Trabajo y personal: control total y se recomienda encarecidamente para dispositivos con otros tipos de activación. Si esta configuración no se selecciona, los usuarios pueden agregar una cuenta de Google gestionada al dispositivo que pude acceder a las aplicaciones de trabajo fuera del perfil de trabajo.
3. Si pretende asignar el tipo de activación Solo espacio de trabajo o Trabajo y personal: control total, seleccione la opción **Aplicar política de EMM**en el dominio G Suite.
4. En BlackBerry UEM, cree cuentas de usuario locales para los usuarios de Android. La dirección de correo de cada cuenta debe coincidir con la dirección de correo de la cuenta de G Suite correspondiente.
5. Asegúrese de que los usuarios conozcan las contraseñas de las cuentas de G Suite.
6. En BlackBerry UEM, asigne un perfil de correo electrónico y aplicaciones de productividad a los usuarios, grupos de usuarios o grupos de dispositivos.

Compatibilidad de las activaciones Android Enterprise con un dominio de Google Cloud

Si ha configurado BlackBerry UEM para conectarse a un dominio de Google Cloud, debe realizar las siguientes tareas antes de que los usuarios puedan activar los dispositivos mediante Android Enterprise.

Antes de empezar: Configure BlackBerry UEM para que sea compatible con Android Enterprise. Cuando se configura BlackBerry UEM para conectarse a un dominio de Google Cloud, debe seleccionar si BlackBerry UEM puede crear cuentas de usuario en el dominio. Esta selección afecta a las tareas que se deben realizar antes de que los usuarios pueden activar los dispositivos con Android Enterprise. Para obtener más información sobre la configuración de BlackBerry UEM para ser compatible con dispositivos Android Enterprise, consulte el contenido de Configuración local o el contenido de Configuración de UEM Cloud.

1. En BlackBerry UEM, agregue las cuentas de usuario del directorio para los usuarios de Android Enterprise.
2. Si elige no permitir a BlackBerry UEM crear cuentas de usuario en el dominio de Google Cloud, deberá crear cuentas de usuario en el dominio de Google Cloud y en BlackBerry UEM. Lleve a cabo una de las siguientes acciones:

- En el dominio de Google Cloud, cree cuentas de usuario para los usuarios de Android Enterprise. Cada dirección de correo debe coincidir con la dirección de correo de la cuenta de usuario de BlackBerry UEM correspondiente. Asegúrese de que los usuarios de Android Enterprise conozcan la contraseña de las cuentas de Google Cloud.
- Utilice Google Apps Directory Sync Tool para sincronizar el dominio de Google Cloud con el directorio de la empresa. Si lo hace, no tendrá que crear manualmente las cuentas de usuario en el dominio de Google Cloud.

3. Si pretende asignar los tipos de activación Solo espacio de trabajo o Trabajo y personal: control total, seleccione la opción **Aplicar política de EMM**en el dominio Google Cloud.

   Esta configuración es necesaria para dispositivos con el tipo de activación Solo espacio de trabajo y Trabajo y personal: control total y se recomienda encarecidamente para dispositivos con otros tipos de activación. Si esta configuración no se selecciona, los usuarios pueden agregar una cuenta de Google gestionada al dispositivo que pude acceder a las aplicaciones de trabajo fuera del perfil de trabajo.
4. En BlackBerry UEM, asigne un perfil de correo electrónico y aplicaciones de productividad a los usuarios, grupos de usuarios o grupos de dispositivos.

Compatibilidad de dispositivos Android Enterprise sin acceso a Google Play

Para activar dispositivos que no tienen acceso a Google Play, los usuarios deben descargar la última versión de BlackBerry UEM Client de una fuente diferente. Los métodos disponibles para descargar UEM Client dependen de la versión del sistema operativo y del tipo de activación:

- Para los dispositivos que se vayan a activar con los tipos de activación Solo espacio de trabajo o Trabajo y personal: control total, deben restablecerse los valores predeterminados de fábrica del dispositivo antes de instalar UEM Client. Para proporcionar la ubicación de descarga al dispositivo, puede incluir la ubicación en un QR Code que el usuario pueda escanear para iniciar la activación o permitir que el dispositivo obtenga información de descarga mediante NFC (por ejemplo, tocando un adhesivo NFC u otro dispositivo).
  - Para obtener información sobre cómo incluir la ubicación de UEM Client en un QR Code, consulte Configuración predeterminada de activación de dispositivos.
  - Para obtener información sobre la programación de un adhesivo NFC, consulte Programación de un adhesivo NFC para activar los dispositivos.
  - Para obtener información sobre el uso de la aplicación BlackBerry UEM Enroll en un dispositivo secundario para proporcionar instrucciones de descarga de UEM Client a través de NFC, consulte la documentación de UEM Enroll. Para utilizar este método, la aplicación BlackBerry UEM Enroll debe estar instalada en un dispositivo con Android 9 y el dispositivo que se vaya a activar debe tener Android 9 o anterior.
- Los dispositivos que vayan a activar con el tipo de activación Trabajo y personal: privacidad de usuario no necesitan restablecerse primero a los valores predeterminados de fábrica. Para estos dispositivos, los usuarios pueden descargar BlackBerry UEM Client desde el sitio de descarga de BlackBerry o desde otra ubicación disponible una vez completada la configuración rápida inicial del dispositivo.

Para descargar el archivo .apk de la versión más reciente de la aplicación UEM Client o UEM Enroll, visite support.blackberry.com/community para leer el artículo 42607.

Para obtener instrucciones sobre cómo activar dispositivos Android Enterprise, consulte Activación de dispositivos con Android

Requisitos

Si quiere activar dispositivos que no tienen acceso a Google Play, compruebe lo siguiente:

Requisito	Descripción
Entorno de BlackBerry UEM	• **Integración con Android Enterprise**: no es necesario que integre UEM con Android Enterprise si solo necesita utilizar dispositivos que no tengan acceso a Google Play. Si necesita compatibilidad con dispositivos con y sin acceso a Google Play, debe integrar el entorno de UEM con Android Enterprise.
Valores predeterminados de activación del dispositivo	Si desea incluir la ubicación de UEM Client en un código QR, compruebe los siguientes valores predeterminados de activación del dispositivo: • Seleccione las opciones **Permitir que el código QR contenga la ubicación del archivo de origen de la aplicación UEM Client** y **Utilizar ubicación predeterminada**. Estas opciones permiten a los usuarios escanear el código QR del correo electrónico de activación para descargar UEM Client desde el sitio de descarga de BlackBerry. Estas opciones solo están disponibles si su entorno de UEM está integrado con Android Enterprise.
Configuración del perfil de activación	Compruebe los siguientes ajustes del perfil de activación: • Desactive la opción **Agregar cuenta de Google Play al espacio de trabajo**. Esta opción solo está disponible si su entorno de UEM está integrado con Android Enterprise. • Si desea activar BlackBerry Secure Connect Plus, seleccione la opción **Al activar dispositivos Android Enterprise, active las funciones premium de UEM como BlackBerry Secure Connect Plus**. Debe cargar la aplicación BlackBerry Connectivity como si fuera una aplicación interna y asignarla a usuarios.
Reglas de políticas de TI	Solo con los usuarios que tengan asignado el tipo de activación Trabajo y personal: privacidad de usuario (Android Enterprise), compruebe lo siguiente en la directiva de TI: • Active la directiva de TI **Permitir instalación de aplicaciones que no sean de Google Play** para permitir la instalación de aplicaciones fuera de Google Play.
Aplicaciones que no son de BlackBerry Dynamics	Para las aplicaciones que no sean de BlackBerry Dynamics, añada las aplicaciones a UEM como si fuesen aplicaciones internas y asígnelas a usuarios. 1. Obtenga los archivos .apk de las aplicaciones que desee asignar. Por ejemplo, para descargar la versión más reciente de la aplicación BlackBerry Connectivity, visite el portal myAccount de BlackBerry. 2. En la consola de gestión de BlackBerry UEM, haga clic en la opción **Aplicaciones** de la barra de menús. 3. Haga clic en > **Aplicaciones internas**. 4. Haga clic en **Examinar** y seleccione el archivo .apk. 5. En el campo **Enviar a**, seleccione **Todos los dispositivos Android**. 6. Anule la selección de **Publicar la aplicación en el dominio de Google**. 7. Haga clic en **Agregar**. 8. Repita los pasos anteriores para cada aplicación que desee agregar. 9. Asigne las aplicaciones a los usuarios. La disposición de la aplicación debe establecerse en **Obligatoria**.

Requisito	Descripción
Aplicaciones de BlackBerry Dynamics	Para las aplicaciones de BlackBerry Dynamics, cargue el archivo de origen de la aplicación interna y asigne la aplicación a usuarios. Lleve a cabo los siguientes pasos para instalar o actualizar aplicaciones internas en dispositivos que no tengan acceso a Google Play: 1. Obtenga los archivos .apk de las aplicaciones de BlackBerry Dynamics que desee asignar. Por ejemplo, para descargar BlackBerry Work, visite support.blackberry.com/community para leer el artículo 42607. 2. En la consola de gestión de BlackBerry UEM, haga clic en la opción **Aplicaciones** de la barra de menús. 3. Haga clic en una aplicación de BlackBerry Dynamics (por ejemplo, BlackBerry Work). 4. Haga clic en la pestaña **Android**. 5. Haga clic en **Agregue archivo de origen de aplicación interna**. 6. Haga clic en **Examinar** y seleccione el archivo .apk. 7. Haga clic en **Agregar**. 8. Haga clic en **Guardar**. 9. Repita los pasos anteriores para cada aplicación que desee agregar. 10. Asigne las aplicaciones a los usuarios. La disposición de la aplicación debe establecerse en **Obligatoria**.
Actualización de la aplicación BlackBerry UEM Client	Para actualizar la aplicación UEM Client en los dispositivos, los usuarios deben descargar manualmente la versión más reciente del archivo .apk e instalarlo. Para obtener más información, visite support.blackberry.com/community para leer el artículo 42607.

Para obtener más información sobre la compatibilidad con los dispositivos Android Enterprise sin acceso a Google Play, visite support.blackberry.com/community para leer el artículo 57492.

Programación de un adhesivo NFC para activar los dispositivos

Los usuarios pueden descargar BlackBerry UEM Client y comenzar la activación del dispositivo si tocan sobre una etiqueta o adhesivo NFC del dispositivo. Este método es una opción para activar dispositivos Solo espacio de trabajo (Android Enterprise) y Trabajo y personal: control total (Android Enterprise) que no tienen acceso a Google Play.

Para permitir que los usuarios activen dispositivos mediante este método, debe programar un adhesivo NFC de un tercero con los valores necesarios para indicar al dispositivo que descargue UEM Client y comience la activación.

Antes de empezar: Necesitará los siguientes elementos:

- Etiqueta o adhesivo NFC
- Un método para programar el adhesivo, como una aplicación Android que pueda leer y escribir en adhesivos NFC.

1. En la consola de gestión, haga clic en **Configuración > Integración externa > Empresa con Android**.
2. En **Inscripción NFC**, haga clic en **Más información**.

3. En un dispositivo con una aplicación que pueda escribir datos en adhesivos NFC, abra la aplicación y permita que esta se conecte al adhesivo que desee programar y agregue la siguiente configuración:
   a) Establezca el tipo de datos NFC en `custom`.
   b) Establezca el tipo de contenido en `application/com.android.managedprovisioning`.
   c) Copie los detalles del cuadro de texto de la consola de gestión en el campo **Configuración** de la aplicación.
4. Escriba la configuración en el adhesivo.

Una vez escrito el programa en el adhesivo, los usuarios deben poder tocar el adhesivo con un dispositivo nuevo o restablecer los ajustes de fábrica para descargar UEM Client y comenzar la activación.

Especificación de la configuración de activación predeterminada

Puede especificar la configuración predeterminada para activar el dispositivo, incluido el tiempo predeterminado durante el que una contraseña de activación es válida antes de que caduque, la longitud de las contraseñas generadas automáticamente que se envían a los usuarios, si se pueden utilizar QR Code para la activación y otras opciones.

Para obtener más información sobre la configuración predeterminada de activación del dispositivo, consulte Configuración predeterminada de activación de dispositivos.

1. En la barra de menús, haga clic en **Configuración > Configuración general**.
2. Haga clic en **Valores predeterminados de activación**.
3. En **Valores predeterminados de la activación del dispositivo** , especifique la contraseña de activación y las opciones de QR Code .
4. Si está administrando Android 9.0 y dispositivos anteriores y desea utilizar el tipo de activación Controles de MDM, active la casilla de verificación **Activar el tipo de activación Controles de MDM para dispositivos Android** para agregar Controles de MDM a la lista de tipos de activación en el perfil de activación.

   Esta opción está activada de forma predeterminada si BlackBerry UEM se ha actualizado desde una versión anterior. Si esta opción está activada, no podrá desactivarla.
5. Seleccione **Utilizar códigos QR para desbloquear aplicaciones de BlackBerry Dynamics** para permitir a los usuarios activar aplicaciones BlackBerry Dynamics con un QR Code. Para obtener más información, consulte Generar claves de acceso, contraseñas de activación o QR Code para BlackBerry Dynamics aplicaciones
6. Seleccione o anule la selección de la casilla para marcar **Activar registro con BlackBerry Infrastructure** para modificar la forma en que los usuarios activan los dispositivos móviles. Si no selecciona esta opción, los usuarios deberán proporcionar la dirección del servidor para BlackBerry UEM al activar dispositivos. Para obtener más información, consulte Activación del registro de usuario con BlackBerry Infrastructure.
7. Para importar o exportar una lista con los ID de los dispositivos aprobados, vaya al archivo .csv de su empresa que contiene una lista de los ID de los dispositivos aprobados. Para obtener más información, consulte Importación o exportación de una lista de ID de los dispositivos aprobados.
8. Haga clic en **Guardar**.

Configuración predeterminada de activación de dispositivos

Configuración	Descripción
Caducidad del periodo de activación	Esta configuración permite especificar el tiempo predeterminado que una contraseña de activación o QR Code son válidos antes de que caduquen. El tiempo puede estar oscilar entre 1 minuto y 30 días.

Configuración	Descripción
El periodo de activación caduca después de la activación del primer dispositivo	Esta configuración especifica si la contraseña de activación o QR Code caducan después de utilizarlos para activar un dispositivo.
Permitir QR Code para la activación de dispositivos	Esta configuración especifica si se puede incluir un QR Code en el mensaje de correo electrónico de activación y mostrarse en BlackBerry UEM Self-Service. Los usuarios pueden escanear QR Code para iniciar la activación del dispositivo. Si no selecciona esta opción, la opción de enviar un QR Code no estará disponible para la plantilla del correo de activación.
Permitir que QR Code contenga la contraseña de activación	Esta configuración especifica si QR Code contiene la contraseña de activación. Si se selecciona esta opción, los usuarios no tienen que escribir una contraseña por separado después de escanear un código QR para activar un dispositivo.
Permitir que el QR Code contenga la ubicación del archivo de origen de la aplicación de UEM Client	Esta configuración especifica si el código de QR Code contiene una ubicación para que el dispositivo descargue el archivo (.apk) de la aplicación de UEM Client. Esta configuración solo es relevante para la activación de dispositivos con Android Enterprise con los tipos de activación Solo espacio de trabajo y Trabajo y personal: control total. Al escanear QR Code con el dispositivo, se inicia la descarga e instalación de BlackBerry UEM Client.
Utilizar ubicación predeterminada	Si configura QR Code para que contenga la ubicación del archivo de origen de UEM Client, seleccione esta opción para especificar que el dispositivo debe obtener el archivo .apk del sitio de descarga de BlackBerry.
Ubicación del archivo de origen de la aplicación de UEM Client	Si configura QR Code para que contenga la ubicación del archivo de origen de UEM Client, esta configuración permite especificar la ubicación desde la que el dispositivo debe descargar el archivo. Puede especificar cualquier ubicación a la que tenga acceso el dispositivo cuando esté configurado con los valores predeterminados de fábrica.
Permitir el uso del nombre de usuario y la contraseña de Microsoft Active Directory	Para los dispositivos activados mediante Samsung Knox Mobile Enrollment, esta configuración especifica si se permite a los usuarios utilizar sus credenciales de Microsoft Active Directory para activar dispositivos.
Enviar notificación de dispositivo activado	Esta configuración especifica si el usuario debe recibir un mensaje de correo electrónico cuando se active un dispositivo.
Longitud de la contraseña de activación generada automáticamente	Esta configuración especifica el número de caracteres de una contraseña generada automáticamente. El valor puede oscilar entre 4 y 16.

Configuración	Descripción
Complejidad de la contraseña generada automáticamente	Esta configuración especifica los tipos de caracteres que debe contener una contraseña generada automáticamente. Las contraseñas pueden incluir los siguientes tipos de caracteres: • Letras minúsculas • Letras mayúsculas • Números • Caracteres especiales o símbolos
Activar el tipo de activación Controles MDM para dispositivos Android	Esta configuración especifica si Controles de MDM se incluye en la lista de tipos de activación de Android del perfil de activación. El tipo de activación Google está obsoleto en los dispositivos con Android 10 y posteriores. Para obtener más información, https://support.blackberry.com/community para leer el artículo 48386. Esta opción está activada de forma predeterminada si BlackBerry UEM se ha actualizado desde una versión anterior. Si esta opción está activada, no podrá desactivarla.
Utilizar códigos QR para desbloquear aplicaciones de BlackBerry Dynamics	Esta configuración especifica si los usuarios pueden activar aplicaciones de BlackBerry Dynamics con un QR Code. Para obtener más información, consulte Generar claves de acceso, contraseñas de activación o QR Code para aplicaciones BlackBerry Dynamics.
Activar registro con BlackBerry Infrastructure	Esta configuración permite activar o desactivar la casilla de verificación **Activar registro con BlackBerry Infrastructure** para modificar la forma en que los usuarios activan dispositivos iOS, iPadOS, macOS y Android. Si elimina la selección de esta opción, los usuarios deberán proporcionar la dirección del servidor para BlackBerry UEM al activar dispositivos. Para obtener más información, consulte Activación del registro de usuario con BlackBerry Infrastructure.

Control de dispositivos con Android con una política de TI

BlackBerry UEM envía una política de TI a cada dispositivo. Puede utilizar una política de TI predeterminada o crear sus propias políticas de TI. Puede crear tantas políticas de TI como desee para diferentes situaciones y distintos usuarios, pero solo una política de TI estará activa en el dispositivo en cada momento.

Las reglas de políticas de TI para Android se basan en la las capacidades del dispositivo y de las opciones de configuración del dispositivo facilitadas por Google y el fabricante del dispositivo. A medida que Google presenta nuevas actualizaciones del sistema operativo con nuevas características y opciones de configuración, se agregan nuevas reglas de políticas de TI a UEM l tan pronto como es posible.

Puede descargar la hoja de cálculo de reglas de políticas de TI que puede ordenar y en la que puede realizar búsquedas. La hoja de cálculo documenta todas las reglas disponibles en UEM, incluido el SO mínimo del dispositivo compatible con la regla.

Entre los comportamientos del dispositivo que puede controlar con una política de TI, se incluyen las siguientes opciones:

- Requisitos de contraseñas del dispositivo
- Permitir funciones del dispositivo, como la cámara y el Bluetooth
- Permitir que aplicaciones de un perfil accedan a los datos de otro perfil
- Restringir funcionalidades solo para aplicaciones y datos del perfil de trabajo.

Para obtener más información sobre el envío de políticas de TI a los dispositivos, consulte el contenido de Administración.

Establecimiento de los requisitos de la contraseña de Android

Hay cuatro grupos de reglas de políticas de TI en las contraseñas Android. El grupo de reglas que se utilice depende del tipo de activación del dispositivo y si se van a establecer requisitos para la contraseña del dispositivo o para la contraseña del espacio de trabajo.

Después de establecer las reglas de contraseña en la política de TI, utilice un perfil de conformidad para aplicar los requisitos de contraseña.

Tipo de activación	Compatibilidad con las reglas para la contraseña
Trabajo y personal: privacidad de usuario (Android Enterprise) y Trabajo y personal: control total (Android Enterprise)	Utilice las reglas para contraseñas globales para establecer los requisitos de la contraseña del dispositivo. Utilice las reglas para la contraseña de los perfiles de trabajo para establecer los requisitos de la contraseña del espacio de trabajo. El dispositivo ignora las reglas de contraseña de Knox.
Solo espacio de trabajo (Android Enterprise)	Utilice las reglas para contraseñas globales para establecer los requisitos de la contraseña del dispositivo. Puesto que el dispositivo solo cuenta con un espacio de trabajo, la contraseña también es la contraseña del espacio de trabajo. El dispositivo ignora el resto de las reglas para la contraseña.

Tipo de activación	Compatibilidad con las reglas para la contraseña
Controles de MDM	Utilice las reglas para contraseñas globales para establecer los requisitos de la contraseña del dispositivo. El dispositivo ignora el resto de las reglas para la contraseña. **Nota:** El tipo de activación Controles de MDM está obsoleto en los dispositivos con Android 10. Para obtener más información, https://support.blackberry.com/community para leer el artículo 48386.
Controles de MDM (Samsung Knox)	Utilice las reglas de contraseña de Knox MDM para establecer los requisitos de contraseña del dispositivo. El dispositivo ignora el resto de las reglas para la contraseña.
Trabajo y personal: privacidad de usuario (Samsung Knox)	No tiene ningún control sobre la contraseña del dispositivo. Utilice las reglas de contraseña Knox Premium - Workspace para establecer los requisitos de contraseña del espacio de trabajo. El dispositivo ignora el resto de las reglas para la contraseña. **Nota:** Los tipos de activación de Samsung Knox quedarán en desuso en una versión futura. Los dispositivos compatibles con Knox Platform for Enterprise se pueden activar mediante los tipos de activación de Android Enterprise. Para obtener más información, visite https://support.blackberry.com/community para leer el artículo 54614.
Trabajo y personal: control total (Samsung Knox)	Utilice las reglas de contraseña de Knox MDM para establecer los requisitos de contraseña del dispositivo. Utilice las reglas de contraseña Knox Premium - Workspace para establecer los requisitos de contraseña del espacio de trabajo. El dispositivo ignora el resto de las reglas para la contraseña.
Solo espacio de trabajo (Samsung Knox)	Utilice las reglas de contraseña Knox Premium - Workspace para establecer los requisitos de contraseña del espacio de trabajo. El dispositivo ignora el resto de las reglas para la contraseña.

Android: reglas de contraseñas globales

Las reglas para la contraseña globales establecen los requisitos de la contraseña del dispositivo para los dispositivos con los siguientes tipos de activación:

- Trabajo y personal: privacidad de usuario (Android Enterprise)
- Trabajo y personal: control total (Android Enterprise)
- Solo espacio de trabajo (Android Enterprise)
- Controles de MDM (sin Samsung Knox)

Nota: El tipo de activación de Controles de MDM está obsoleto en los dispositivos con Android 10. Para obtener más información, https://support.blackberry.com/community y lea el artículo 48386.

Regla	Descripción
Requisitos de la contraseña	Especifique los requisitos mínimos de la contraseña. Puede elegir una de las siguientes opciones: • Sin especificar: no se requiere contraseña • Algunos: el usuario deberá establecer una contraseña pero no habrá requisitos relacionados con la longitud o la calidad • Numérica: la contraseña deberá incluir al menos un número • Alfabética: la contraseña deberá incluir al menos una letra • Alfanumérica: la contraseña deberá incluir al menos una letra y un número • Complejos: permite establecer requisitos específicos para los diferentes tipos de caracteres
Número máximo de intentos de contraseña fallidos	Especifique el número de veces que un usuario puede introducir una contraseña incorrecta antes de que el dispositivo se desactive o se eliminen sus datos. Se eliminan los dispositivos con el tipo de activación "Controles de MDM". Se desactivarán los dispositivos con los tipos de activación "Trabajo y personal: privacidad de usuario " y "Trabajo y personal: privacidad de usuario (Premium)" y se eliminará el perfil de trabajo.
Bloqueo de tiempo de inactividad máximo	Especifique el número máximo de minutos de inactividad del usuario que deben transcurrir antes de que el dispositivo o el espacio de trabajo se bloqueen. En dispositivos con Android con un perfil de trabajo, el espacio de trabajo también se bloquea. Los usuarios pueden establecer un periodo más breve en el dispositivo. Esta regla se ignora si no se necesita contraseña.
Tiempo de espera de caducidad de la contraseña	Especifique la cantidad máxima de tiempo que puede utilizarse la contraseña. Una vez transcurrida la cantidad de tiempo especificada, el usuario deberá establecer una nueva contraseña. Si se establece en 0, la contraseña no caduca.
Restricción del historial de contraseñas	Especifique el número máximo de contraseñas anteriores que el dispositivo debe comprobar para evitar que un usuario vuelva a utilizar una contraseña numérica, alfabética, alfanumérica o compleja reciente. Si se establece en 0, el dispositivo no comprueba las contraseñas anteriores.
Longitud mínima de la contraseña:	Especifique el número mínimo de caracteres necesarios en una contraseña numérica, alfabética, alfanumérica o compleja.
Número mínimo de letras mayúsculas requerido en la contraseña	Especifique el número mínimo de letras mayúsculas que debe contener una contraseña compleja.
Número mínimo de letras minúsculas requerido en la contraseña	Especifique el número mínimo de letras minúsculas que debe contener una contraseña compleja.
Número mínimo de letras requerido en la contraseña	Especifique el número mínimo de letras que debe contener una contraseña compleja.

Regla	Descripción
Número mínimo de caracteres no alfabéticos en la contraseña	Especifique el número mínimo de caracteres no alfabéticos (números o símbolos) que debe contener una contraseña compleja.
Mínimo de dígitos numéricos requeridos en la contraseña	Especifique el número mínimo de números que debe contener una contraseña compleja.
Número mínimo de símbolos requerido en la contraseña	Especifique el número mínimo de caracteres complejos que debe contener una contraseña compleja.

Para obtener más información acerca de las reglas de contraseñas de las políticas de TI, descargue la hoja de cálculo de referencia de políticas.

Android: reglas para las contraseñas de los perfiles de trabajo

Las reglas para las contraseñas de los perfiles de trabajo establecen los requisitos de la contraseña del espacio de trabajo para los dispositivos con los siguientes tipos de activación:

- Trabajo y personal: privacidad de usuario (Android Enterprise)
- Trabajo y personal: control total (Android Enterprise)

Regla	Descripción
Requisitos de la contraseña	Especifique los requisitos mínimos de la contraseña del espacio de trabajo. Puede elegir una de las siguientes opciones: • Algunos: el usuario deberá establecer una contraseña pero no habrá requisitos relacionados con la longitud o la calidad • Numérica: la contraseña deberá incluir al menos un número • Alfabética: la contraseña deberá incluir al menos una letra • Alfanumérica: la contraseña deberá incluir al menos una letra y un número • Complejos: permite establecer requisitos específicos para los diferentes tipos de caracteres • Complejos, numérica: la contraseña debe contener caracteres numéricos con secuencias no repetidas (4444) ni ordenadas (1234, 4321, 2468). • Parámetros biométricos débiles: la contraseña permite la tecnología de reconocimiento biométrico de seguridad baja. Para dispositivos con BlackBerry alimentados por Android, puede forzar el espacio de trabajo y las contraseñas de los dispositivos para que sean diferentes mediante la regla "Forzar el espacio de trabajo y las contraseñas de los dispositivos para que sean diferentes" de los dispositivos con BlackBerry.
Número máximo de intentos de contraseña fallidos	Especifique el número de veces que un usuario puede introducir una contraseña incorrecta del espacio de trabajo para que se desactive el dispositivo y el perfil de trabajo se elimine.

Regla	Descripción
Bloqueo de tiempo de inactividad máximo	Especifique cuántos minutos de inactividad del usuario deben transcurrir como máximo para que el dispositivo y el espacio de trabajo se bloqueen. Si configura esta regla y la regla "Bloqueo de tiempo de inactividad máximo" de Android global, el dispositivo y el espacio de trabajo se bloquean cuando el contador de cualquiera de las reglas llega a su fin. Los usuarios pueden establecer un periodo más breve en el dispositivo.
Tiempo de espera de caducidad de la contraseña	Especifique la cantidad máxima de tiempo que puede utilizarse la contraseña del espacio de trabajo. Una vez transcurrida la cantidad de tiempo especificada, el usuario deberá establecer una nueva contraseña del espacio de trabajo. Si se establece en 0, la contraseña no caduca.
Restricción del historial de contraseñas	Especifique el número máximo de contraseñas anteriores del espacio de trabajo que el dispositivo debe comprobar para evitar que un usuario vuelva a utilizar una contraseña numérica, alfabética, alfanumérica o compleja reciente. Si se establece en 0, el dispositivo no comprueba las contraseñas anteriores.
Longitud mínima de la contraseña:	Especifique el número mínimo de caracteres necesarios en una contraseña del espacio de trabajo numérica, alfabética, alfanumérica o compleja.
Número mínimo de letras mayúsculas requerido en la contraseña	Especifique el número mínimo de letras en mayúscula que debe contener la contraseña compleja del espacio de trabajo.
Número mínimo de letras minúsculas requerido en la contraseña	Especifique el número mínimo de letras en minúscula que debe contener la contraseña compleja del espacio de trabajo.
Número mínimo de letras requerido en la contraseña	Especifique el número mínimo de letras que debe contener la contraseña compleja del espacio de trabajo.
Número mínimo de caracteres no alfabéticos en la contraseña	Especifique el número mínimo de caracteres no alfabéticos (números o símbolos) que debe contener una contraseña compleja del espacio de trabajo.
Mínimo de dígitos numéricos requeridos en la contraseña	Especifique el número mínimo de números que debe contener la contraseña compleja del espacio de trabajo.
Número mínimo de símbolos requerido en la contraseña	Especifique el número mínimo de caracteres no alfanuméricos que debe contener una contraseña compleja del espacio de trabajo.
Forzar el uso de contraseñas distintas para el perfil de trabajo y el dispositivo	Especifique si los usuarios deben establecer contraseñas diferentes para el dispositivo y el perfil de trabajo. Cuando las contraseñas son las mismas, al desbloquear el dispositivo se desbloquea el perfil de trabajo.

Para obtener más información acerca de las reglas de contraseñas de las políticas de TI, descargue la hoja de cálculo de referencia de políticas.

Control de dispositivos Android con perfiles

BlackBerry UEM incluye varios modos que puede utilizar para controlar diversos aspectos de la funcionalidad del dispositivo. Entre los más utilizados, se incluyen los siguientes perfiles:

Nombre de perfil	Descripción	Configuración de
Activación	Especifica las opciones de activación de los dispositivos para los usuarios, como el tipo de activación, el método y el número y tipos de dispositivos que un usuario puede activar.	Creación de un perfil de activación
Wi-Fi	Especifica la configuración de los dispositivos que puede conectar a su red de trabajo Wi-Fi.	Creación de un perfil de Wi-Fi
VPN	Especifica la configuración de los dispositivos para poder conectarse a una red VPN de trabajo.	Crear un perfil VPN
Proxy	Especifica cómo pueden usar un servidor proxy los dispositivos para acceder a servicios web en Internet o en una red de trabajo.	Creación de un perfil de proxy
Correo	Especifica cómo se conectan los dispositivos al servidor de correo de trabajo y cómo sincronizan los mensajes de correo, las entradas del calendario y los datos del organizador. Si instala y configura BlackBerry Work en los dispositivos, no tendrá que configurar un perfil de correo electrónico.	Crear un perfil de correo electrónico
BlackBerry Dynamics	Permite que los dispositivos accedan a aplicaciones de BlackBerry Dynamics como BlackBerry Work, BlackBerry Access y BlackBerry Connect.	Creación de un perfil de BlackBerry Dynamics
Conectividad de BlackBerry Dynamics	Define las conexiones de red, los dominios de Internet, los rangos de dirección IP y los servidores de aplicaciones a los que los dispositivos se pueden conectar cuando se usan aplicaciones de BlackBerry Dynamics.	Creación de un perfil de conectividad de BlackBerry Dynamics
Conformidad	Define las condiciones de dispositivo no aceptables en la empresa y establece las acciones de cumplimiento.	Creación de un perfil de cumplimiento
Conectividad de la empresa	Especifica si los dispositivos pueden utilizar BlackBerry Secure Connect Plus.	Activar BlackBerry Secure Connect Plus

Nombre de perfil	Descripción	Configuración de
Certificado de CA	Especifica un certificado de CA que los dispositivos pueden utilizar para establecer una conexión de confianza con una red o servidor de trabajo.	Creación de un perfil de certificado de CA
Credencial de usuario	Especifica cómo obtienen los dispositivos certificados de clientes que se usan para autenticar con una red o servidor de trabajo.	Creación de un perfil de credenciales de usuario
SCEP	Especifica el servidor SCEP que los dispositivos pueden utilizar para obtener un certificado de cliente utilizado para autenticar con una red o servidor de trabajo.	Crear un perfil SCEP

Para obtener más información sobre el envío de perfiles a los dispositivos, consulte el contenido de Administración.

Referencia de perfiles: dispositivos con Android

En la siguiente tabla se enumeran todos los perfiles de BlackBerry UEM compatibles con dispositivos con Android:

Nombre de perfil	Descripción	Configurar
Política		
Activación	Especifica las opciones de activación de los dispositivos para los usuarios, como el tipo de activación y el número y tipos de dispositivos.	Creación de un perfil de activación
BlackBerry Dynamics	Permite que los dispositivos accedan a aplicaciones de BlackBerry Dynamics como BlackBerry Work, BlackBerry Access y BlackBerry Connect.	Creación de un perfil de BlackBerry Dynamics
Modo de bloqueo de la aplicación	Especifique una aplicación única para ejecutar en los dispositivos Solo dispositivos con Samsung Knox activados con MDM	Crear un perfil de modo de bloqueo de la aplicación
Enterprise Management Agent	Especifica cuándo los dispositivos se conectan a BlackBerry UEM en busca de actualizaciones de aplicaciones o de configuración cuando una notificación de inserción no esté disponible.	Creación de un perfil de Enterprise Management Agent
Conformidad		

Nombre de perfil	Descripción	Configurar
Conformidad	Define las condiciones de dispositivo no aceptables en la empresa y establece las acciones de conformidad.	Creación de un perfil de conformidad
Conformidad (BlackBerry Dynamics)	Esta es un perfil de solo lectura que muestra los ajustes de conformidad importados de Good Control a una instancia de BlackBerry UEM local.	Gestión de perfiles de conformidad de BlackBerry Dynamics
Requisitos de informe especial del dispositivo	Define la versión de software que los dispositivos deben tener instalada y especifica un periodo de actualización para las aplicaciones que se ejecutan en primer plano.	Crear un perfil de requisitos de versión de software del dispositivo
Correo, calendario y contactos		
Correo	Especifica cómo se conectan los dispositivos al servidor de correo de trabajo y cómo sincronizan los mensajes de correo, las entradas del calendario y los datos del organizador mediante Exchange ActiveSync o IBM Notes Traveler.	Crear un perfil de correo electrónico
IMAP/correo electrónico POP3	Especifica la forma de conexión de los dispositivos a un servidor de correo electrónico IMAP o POP3 y cómo sincronizar mensajes de correo electrónico.	Creación de un perfil de correo IMAP/POP3
Enlace	Especifica los servidores de Microsoft Exchange que se deben utilizar para un enlace automático.	Creación de un perfil de enlace
Redes y conexiones		
Wi-Fi	Especifica la forma de conexión de los dispositivos a una red Wi-Fi de trabajo.	Creación de un perfil de Wi-Fi
VPN	Especifica la forma de conexión de los dispositivos a una red VPN de trabajo.	Crear un perfil VPN
Proxy	Especifica cómo pueden usar un servidor proxy los dispositivos para acceder a servicios web en Internet o en una red de trabajo.	Creación de un perfil de proxy

Nombre de perfil	Descripción	Configurar
Conectividad de la empresa	Especifica el método de conexión de los dispositivos con los recursos de su empresa mediante la conectividad de la empresa. Para los dispositivos Android Enterprise y Samsung Knox Workspace, el perfil de conectividad de la empresa especifica si los dispositivos pueden usar BlackBerry Secure Connect Plus.	Activar BlackBerry Secure Connect Plus
Conectividad de BlackBerry Dynamics	Define las conexiones de red, los dominios de Internet, los rangos de dirección IP y los servidores de aplicaciones a los que los dispositivos se pueden conectar cuando se usan aplicaciones de BlackBerry Dynamics.	Creación de un perfil de conectividad de BlackBerry Dynamics
BlackBerry 2FA	Permite la autenticación de dos factores para los usuarios y especifica la configuración de las funciones de autenticación previa y de autorrescate.	Crear un perfil de BlackBerry 2FA
Perfil de nombre de punto de acceso	Le permite especificar los APN para que los dispositivos los utilicen para conectarse a los operadores.	Creación de un perfil de nombre de punto de acceso
Protección		
Protección de aplicaciones de Microsoft Intune	Le permite gestionar las aplicaciones protegidas por Microsoft Intune.	Creación de un perfil de protección de aplicación de Microsoft Intune
Servicio de ubicación	Le permite solicitar la ubicación de los dispositivos y ver las ubicaciones aproximadas en un mapa.	Creación de un perfil de servicio de ubicación
No molestar	Le permite bloquear las notificaciones de BlackBerry Work for Android durante los días y horas fuera del trabajo que defina.	Crear un perfil de no molestar
Personalizada		
Dispositivo	Permite configurar la información que aparece en los dispositivos.	Creación de un perfil de dispositivo
Certificados		
Certificado de CA	Especifica un certificado de CA que los dispositivos pueden utilizar para establecer una conexión de confianza con una red o servidor de trabajo.	Creación de un perfil de certificado de CA

Nombre de perfil	Descripción	Configurar
Certificado compartido	Especifica un certificado de cliente que los dispositivos puedan utilizar para autenticar usuarios en una red o servidor de trabajo.	Creación de un perfil de certificado compartido
Credencial de usuario	Especifica la conexión de CA que los dispositivos pueden utilizar para obtener un certificado de cliente utilizado para autenticar con una red o servidor de trabajo.	Creación de un perfil de credenciales de usuario
SCEP	Especifica el servidor SCEP que los dispositivos pueden utilizar para obtener un certificado de cliente utilizado para autenticar con una red o servidor de trabajo.	Crear un perfil SCEP
CRL	Especifique las configuraciones CRL que BlackBerry UEM puede utilizar para comprobar el estado de los certificados. Dispositivos BlackBerry con tecnología Android solamente	Creación de un perfil CRL
Perfil de asignación de certificados	Especifica los certificados de cliente que deben utilizar las aplicaciones.	Creación de un perfil de asignación de certificados

Administración de aplicaciones en dispositivos con Android

Puede crear una biblioteca de aplicaciones que desee administrar y supervisar en los dispositivos. Para los dispositivos con Android Enterprise solo las aplicaciones que permita se instalarán en el perfil de trabajo. BlackBerry UEM proporciona las siguientes opciones para gestionar las aplicaciones en los dispositivos con Android:

- Asignar aplicaciones públicas desde Google Play según sea obligatorio u opcional en los dispositivos.
- Cargar aplicaciones personalizadas a UEM e implementarlas como aplicaciones opcionales u obligatorias.
- Preconfigurar la configuración de las aplicaciones, como la configuración de conexión, cuando la aplicación lo permita.
- Bloquear a los usuarios el acceso a aplicaciones.
- Configurar las aplicaciones de BlackBerry Dynamics públicas, ISV y personalizadas para permitir que los usuarios accedan a los recursos de trabajo.
- Conectar UEM a Microsoft Intune para establecer políticas de protección de la aplicación Intune desde dentro de la consola de administración de UEM para implementar y administrar aplicaciones de Office 365.
- Ver la lista de aplicaciones personales instaladas en los dispositivos.
- Permitir que los usuarios evalúen y revisen aplicaciones de otros usuarios de su entorno.

Comportamiento de la aplicación en los dispositivos Android Enterprise

En los dispositivos habilitados para utilizar BlackBerry Dynamics, el catálogo de aplicaciones de trabajo aparece en BlackBerry Dynamics Launcher si ha asignado el derecho "Función: tienda de aplicaciones de BlackBerry" al usuario. Para obtener más información, consulte Agregar el catálogo de aplicaciones de trabajo a BlackBerry Dynamics Launcher.

Para dispositivos Android Enterprise, se produce el comportamiento siguiente:

Tipo de aplicación	Cuando la aplicación está asignada a un usuario	Cuando se actualizan las aplicaciones	Cuando la aplicación no está asignada a un usuario	Cuando se elimina el dispositivo de BlackBerry UEM
Aplicaciones públicas con una disposición obligatoria	Las aplicaciones se instalan automáticamente.	Las aplicaciones se actualizan automáticamente.	Las aplicaciones se eliminan automáticamente del dispositivo.	El perfil de trabajo y las aplicaciones de trabajo asignadas se eliminan del dispositivo.
Aplicaciones públicas con una disposición opcional	El usuario puede elegir si desea instalar las aplicaciones. Las aplicaciones aparecen en Google Play for Work.	Google Play for Work notifica a los usuarios acerca de las actualizaciones.	Las aplicaciones se eliminan automáticamente del dispositivo.	El perfil de trabajo y las aplicaciones de trabajo asignadas se eliminan del dispositivo.

Tipo de aplicación	Cuando la aplicación está asignada a un usuario	Cuando se actualizan las aplicaciones	Cuando la aplicación no está asignada a un usuario	Cuando se elimina el dispositivo de BlackBerry UEM
Aplicaciones internas con una disposición obligatoria alojadas en BlackBerry UEM	Solo es compatible con dispositivos Solo espacio de trabajo. Las aplicaciones se instalan automáticamente.	Solo es compatible con dispositivos Solo espacio de trabajo. Las aplicaciones se instalan automáticamente.	Las aplicaciones se eliminan automáticamente del dispositivo.	Las aplicaciones se eliminan automáticamente del dispositivo.
Aplicaciones internas con una disposición opcional alojadas en BlackBerry UEM	El usuario puede elegir si desea instalar las aplicaciones. Las aplicaciones aparecen en Google Play for Work.	Google Play for Work notifica a los usuarios acerca de las actualizaciones.	Las aplicaciones se eliminan automáticamente del dispositivo.	El perfil de trabajo y las aplicaciones de trabajo asignadas se eliminan del dispositivo.
Aplicaciones internas con una disposición obligatoria alojadas en Google Play	Las aplicaciones se instalan automáticamente en el dispositivo.	Google Play for Work notifica a los usuarios acerca de las actualizaciones.	Las aplicaciones se eliminan automáticamente del dispositivo.	El perfil de trabajo y las aplicaciones de trabajo asignadas se eliminan del dispositivo.
Aplicaciones internas con una disposición opcional alojadas en Google Play	El usuario puede elegir si desea instalar las aplicaciones. Las aplicaciones aparecen en Google Play for Work.	Google Play for Work notifica a los usuarios acerca de las actualizaciones.	Las aplicaciones se eliminan automáticamente del dispositivo.	El perfil de trabajo y las aplicaciones de trabajo asignadas se eliminan del dispositivo.

Puede especificar el comportamiento de actualización para las aplicaciones que se ejecutan en primer plano en el perfil de requisitos de SR del dispositivo.

Activación de dispositivos con Android

Los pasos que deben seguir los usuarios para instalar BlackBerry UEM Client e iniciar la activación del dispositivo Android dependen de diversos factores, entre ellos, la versión del sistema operativo Android, el fabricante del dispositivo, cómo utiliza su empresa los servicios de Google, el tipo de activación especificado en el perfil de activación del dispositivo y las preferencias de su empresa. Puede proporcionar a los usuarios instrucciones en el correo de activación que BlackBerry UEM envía a los usuarios. Para obtener más información, consulte Plantillas de correo electrónico.

Los dispositivos Android Enterprise admiten varios métodos para que los usuarios inicien el proceso de activación:

Método de activación	Descripción
Instalar UEM Client desde Google Play	Los dispositivos que se vayan a activar con el tipo de activación Trabajo y personal: privacidad de usuario no necesitan restablecerse a los valores predeterminados de fábrica antes de la activación. Para activar estos dispositivos, los usuarios pueden descargar UEM Client en su dispositivo desde Google Play. Para obtener más información, consulte Activación de un dispositivo Android Enterprise con el tipo de activación de Trabajo y personal: privacidad de usuario.
El usuario descarga UEM Client desde el sitio de descarga de BlackBerry	En situaciones en las que los usuarios de Android no tengan acceso a Google Play, para aquellos dispositivos que se vayan a activar con el tipo de activación Trabajo y personal: privacidad de usuario, los usuarios pueden descargar el archivo .apk de UEM Client del sitio de descarga de BlackBerry o pueden descargar el archivo de BlackBerry y colocarlo en una ubicación a la que los usuarios puedan acceder. Para obtener más información, visite support.blackberry.com/community para leer el artículo 42607.
Introducir las credenciales de dominio de Google durante la configuración del dispositivo	Si BlackBerry UEM está conectado al dominio de G Suite o Google Cloud de la empresa, para activar los dispositivos a los que se ha asignado el tipo de activación Solo espacio de trabajo o Trabajo y personal: control total, cuando los usuarios introducen sus credenciales de Google de trabajo durante la configuración del dispositivo, el dispositivo descarga UEM Client e inicia el proceso de activación. Para obtener más información, consulte Activación de un dispositivo Android Enterprise cuando BlackBerry UEM se conecta a un dominio de Google.
Escanear un QR Code que contenga la ubicación de descarga de UEM Client	BlackBerry UEM permite incluir la ubicación de descarga de UEM Client en el QR Code agregado al correo electrónico de activación enviado a los usuarios. Para activar dispositivos que tengan asignado el tipo de activación Solo espacio de trabajo o Trabajo y personal: control total, los usuarios pueden tocar la pantalla de inicio del dispositivo siete veces para abrir un lector de QR Code y escanear el QR Code. Es posible que algunos fabricantes de dispositivos no admitan esta función. Para obtener más información, consulte Activar un dispositivo Android Enterprise con el tipo de activación Trabajo y personal: control total mediante una cuenta de Google Play gestionada.

Método de activación	Descripción
Introducir el hashtag afw#blackberry durante la configuración del dispositivo	Si su empresa utiliza cuentas de Google Play gestionadas para conectarse a los servicios de Google, para activar dispositivos que tengan asignado el tipo de activación Solo espacio de trabajo o Trabajo y personal: control total, en la pantalla donde los usuarios introducen sus credenciales de Google durante la configuración del dispositivo, pueden escribir `afw#blackberry` en su lugar para iniciar la descarga de UEM Client y comenzar el proceso de activación. Para dispositivos con Android 11 y posterior, `afw#blackberry` solo es compatible con el tipo de activación de Solo espacio de trabajo. Para dispositivos con Android 8 y 9, `afw#blackberry` ya no es compatible. Para obtener más información, consulte Activar un dispositivo Android Enterprise con el tipo de activación Solo espacio de trabajo mediante una cuenta de Google Play gestionada.
Tocar un adhesivo NFC o un dispositivo secundario con la aplicación de BlackBerry UEM Enroll que se haya programado con la ubicación de descarga de UEM Client	Puede programar un adhesivo NFC o configurar un dispositivo secundario que tenga instalada la aplicación de UEM Enroll. Para activar dispositivos que tengan asignado el tipo de activación Solo espacio de trabajo o Trabajo y personal: control total, los usuarios pueden tocar el adhesivo NFC o el dispositivo secundario para iniciar la descarga de UEM Client. Se puede utilizar el mismo dispositivo secundario o adhesivo NFC para activar dispositivos para varios usuarios. Para obtener más información, consulte Activación de un dispositivo Android Enterprise sin acceso a Google Play.
Aprovisionamiento automático de Android o Samsung Knox Mobile Enrollment	El aprovisionamiento automático de Android permite implementar un gran número de dispositivos Android Enterprise a la vez. Knox Mobile Enrollment permite implementar un gran número de dispositivos Samsung Knox con activaciones de Android Enterprise. Para utilizar esta opción, los dispositivos deben estar preparados para el aprovisionamiento automático o Knox Mobile Enrollment cuando estos se adquieran de un distribuidor autorizado. Para obtener más información, consulte Configuración de la compatibilidad para el aprovisionamiento automático de Android o Active varios dispositivos mediante Knox Mobile Enrollment.

Cada opción para descargar UEM Client e iniciar la activación del dispositivo solo es compatible con determinados tipos de activación. Para los tipos de activación Solo espacio de trabajo y Trabajo y personal: control total, las opciones compatibles también dependen de cómo utilice la empresa los servicios de Google.

Tipo de activación	Trabajo y personal: privacidad de usuario	Trabajo y personal: control total			Solo espacio de trabajo		
Método		**Dominio de Google**	**Google Play gestionado**	**Sin acceso a Google**	**Dominio de Google**	**Google Play gestionado**	**Sin acceso a Google**
Instalar UEM Client desde Google Play o descarga del usuario	Sí	No	No	No	No	No	No
Credenciales de dominio de Google	Sí	Sí	No	No	Sí	No	No
Escanear QR Code	No	Sí	Sí	Sí	Sí	Sí	Sí
Hashtag afw#blackberry	No	No	Android 10	No	No	Android 10 y posteriores	No
Tocar el adhesivo NFC o el dispositivo secundario	No	Sí	Sí	Sí	Sí	Sí	Sí
Aprovisionamie automático de Android/Samsu Knox Mobile Enrollment	No	Sí	Sí	Sí	Sí	Sí	Sí

Tipos de activación: Dispositivos Android

Para los dispositivos con Android, puede seleccionar varios tipos de activación y clasificarlos para asegurarse de que BlackBerry UEM asigne el tipo de activación más adecuada para el dispositivo. Por ejemplo, si clasifica "Trabajo y personal: privacidad de usuario (Samsung Knox)" en primer lugar y "Trabajo y personal: privacidad de usuario (Android Enterprise)" en segundo lugar, los dispositivos compatibles con Samsung Knox Workspace reciben el primer tipo de activación y los dispositivos que no lo son reciben el segundo.

Los tipos de activación de Android se organizan en las siguientes tablas:

- Dispositivos Android Enterprise
- Dispositivos Android sin un perfil de trabajo
- Dispositivos Samsung Knox Workspace

Dispositivos Android Enterprise

Los siguientes tipos de activación solo se aplican a dispositivos con Android Enterprise.

Tipo de activación	Descripción
Trabajo y personal: privacidad de usuario (Android Enterprise con perfil de trabajo)	Este tipo de activación conserva la privacidad de los datos personales, pero le permite administrar los datos de trabajo con comandos y reglas de políticas de TI. Este tipo de activación crea un perfil de trabajo en el dispositivo que separa los datos de trabajo y los datos personales. Los datos personales y los datos de trabajo están protegidos mediante el cifrado y la autenticación de contraseña. Para activar el soporte de BlackBerry Secure Connect Plus y Knox Platform for Enterprise, debe seleccionar la opción **Al activar dispositivos Android Enterprise, active las funciones premium de UEM como BlackBerry Secure Connect Plus** en el perfil de activación. Los usuarios no tienen que conceder permisos de administrador a BlackBerry UEM Client.
Trabajo y personal: control total (dispositivo Android Enterprise completamente gestionado con perfil de trabajo)	Este tipo de activación le permite administrar todo el dispositivo con comandos y reglas de políticas de TI. Este tipo de activación crea un perfil de trabajo en el dispositivo que separa los datos de trabajo y los datos personales. Los datos en el espacio de trabajo estarán protegidos mediante cifrado y un método de autenticación como una contraseña, un PIN, un patrón o una huella digital. Este tipo de activación es compatible con el registro de actividad del dispositivo (SMS, MMS y llamadas telefónicas) en archivos de registro de BlackBerry UEM. Tras la activación, los dispositivos con el tipo de activación Trabajo y personal: control total solo tienen un conjunto limitado de aplicaciones estándar preinstaladas, como Cámara, Teléfono y Ajustes, en el espacio personal. La lista de aplicaciones preinstaladas conservada depende del proveedor de dispositivos y de la versión del sistema operativo. Para activar el soporte de BlackBerry Secure Connect Plus y Knox Platform for Enterprise, debe seleccionar la opción **Al activar dispositivos Android Enterprise, active las funciones premium de UEM como BlackBerry Secure Connect Plus** en el perfil de activación. Este tipo de activación requiere que el dispositivo se restablezca a la configuración predeterminada de fábrica antes de la activación. Si se elimina BlackBerry UEM Client o se borra el perfil de trabajo del dispositivo, este se restablece automáticamente en los valores predeterminados de fábrica. Durante la activación los usuarios deberán conceder los permisos de administrador a BlackBerry UEM Client.

Tipo de activación	Descripción
Solo espacio de trabajo (dispositivo Android Enterprise completamente gestionado)	Este tipo de activación le permite administrar todo el dispositivo con comandos y reglas de políticas de TI. Este tipo de activación requiere que el usuario restablezca la configuración predeterminada de fábrica del dispositivo antes de realizar la activación. El proceso de activación instala un perfil de trabajo y no instala ningún perfil personal. El usuario debe crear una contraseña para acceder al dispositivo. Todos los datos del dispositivo estarán protegidos mediante cifrado y un método de autenticación como una contraseña. Durante la activación el dispositivo instala automáticamente BlackBerry UEM Client y le concede permisos de administrador. Los usuarios no pueden revocar los permisos de administrador o desinstalar la aplicación. Tras la activación, los dispositivos con el tipo de activación Solo espacio de trabajo solo tienen un conjunto limitado de aplicaciones estándar preinstaladas, como Cámara, Teléfono y Ajustes, además de aquellas aplicaciones que haya asignado con una disposición obligatoria. La lista de aplicaciones preinstaladas conservada depende del proveedor de dispositivos y de la versión del sistema operativo. Para activar el soporte de BlackBerry Secure Connect Plus y Knox Platform for Enterprise, debe seleccionar la opción **Al activar dispositivos Android Enterprise, active las funciones premium de UEM como BlackBerry Secure Connect Plus** en el perfil de activación. Este tipo de activación requiere que el dispositivo se restablezca a la configuración predeterminada de fábrica antes de la activación. Si se elimina BlackBerry UEM Client o se borra el perfil de trabajo del dispositivo, este se restablece automáticamente en los valores predeterminados de fábrica.

Dispositivos Android sin un perfil de trabajo

Los siguientes tipos de activación se aplican a todos los dispositivos con Android.

Tipo de activación	Descripción
Controles de MDM	Este tipo de activación le permite administrar el dispositivo con comandos y reglas de políticas de TI. No se crea un espacio de trabajo separado en el dispositivo y no hay seguridad adicional para los datos de trabajo. **Nota:** Este tipo de activación está obsoleto en los dispositivos con Android 10. Los intentos de activar dispositivos con Android 10 y versiones posteriores con el tipo de activación de Controles de MDM fallarán. Para obtener más información, https://support.blackberry.com/community para leer el artículo 48386. Si el dispositivo es compatible con Knox MDM, este tipo de activación se aplica a las reglas de políticas de TI de Knox MDM. Si no desea aplicar las reglas de políticas de Knox MDM, desmarque la casilla de verificación **Activar Samsung KNOX en dispositivos Samsung que tienen el tipo de activación Controles de MDM asignado**. Durante la activación los usuarios deberán conceder los permisos de administrador a BlackBerry UEM Client.

Tipo de activación	Descripción
Privacidad del usuario	Puede utilizar el tipo de activación Privacidad del usuario para proporcionar un control básico de los dispositivos, con la inclusión de la administración de aplicaciones de trabajo, a la vez que se garantiza la privacidad de los datos personales de los usuarios. Con este tipo de activación, no se instalan contenedores independientes en el dispositivo. Para proporcionar seguridad a los datos del trabajo, puede instalar aplicaciones de BlackBerry Dynamics. Los dispositivos activados con Privacidad del usuario pueden utilizar servicios como Find my Phone y Root Detection, aunque los administradores no pueden controlar las políticas de los dispositivos. También puede utilizar el tipo de activación Privacidad del usuario para activar dispositivos con Chrome OS y poder instalar y administrar las aplicaciones de BlackBerry Dynamics de Android.
Registro del dispositivo solo para BlackBerry 2FA	Este tipo de activación es compatible con la solución de BlackBerry 2FA para dispositivos que BlackBerry UEM no administra. Este tipo de activación no proporciona ningún control o administración de dispositivos, pero permite que los dispositivos utilicen la característica BlackBerry 2FA. Para utilizar este tipo de activación, también debe asignar el perfil BlackBerry 2FA a los usuarios. Cuando se activa un dispositivo, puede ver información limitada de este en la consola de gestión y desactivar el dispositivo mediante un comando. Este tipo de activación solo es compatible con usuarios de Microsoft Active Directory. Para obtener más información, consulte el contenido de BlackBerry 2FA.

Dispositivos Samsung Knox Workspace

Los siguientes tipos de activación solo se aplican a dispositivos Samsung compatibles con Knox Workspace.

Nota: Los tipos de activación de Samsung Knox quedarán en desuso en una versión futura. Los dispositivos compatibles con Knox Platform for Enterprise se pueden activar mediante los tipos de activación de Android Enterprise. Para obtener más información, visite https://support.blackberry.com/community para leer el artículo 54614.

Tipo de activación	Descripción
Trabajo y personal: privacidad de usuario - (Samsung Knox)	Este tipo de activación conserva la privacidad de los datos personales, pero le permite administrar los datos de trabajo con comandos y reglas de políticas de TI. Este tipo de activación no admite las reglas de políticas de TI de Knox MDM. Este tipo de activación crea un espacio de trabajo independiente en el dispositivo y el usuario debe crear una contraseña para acceder al espacio de trabajo. Los datos en el espacio de trabajo estarán protegidos mediante cifrado y un método de autenticación como una contraseña, un PIN, un patrón o una huella digital. El usuario también debe crear una contraseña de bloqueo de pantalla para proteger la totalidad del dispositivo y no podrá utilizar el modo de depuración USB. Durante la activación los usuarios deberán conceder los permisos de administrador a BlackBerry UEM Client.

Tipo de activación	Descripción
Trabajo y personal: control total (Samsung Knox)	Este tipo de activación permite administrar todo el dispositivo con comandos y reglas de políticas de TI de Knox MDM y Knox Workspace. Este tipo de activación crea un espacio de trabajo independiente en el dispositivo y el usuario debe crear una contraseña para acceder al espacio de trabajo. Los datos en el espacio de trabajo estarán protegidos mediante cifrado y un método de autenticación como una contraseña, un PIN, un patrón o una huella digital. Este tipo de activación es compatible con el registro de actividad del dispositivo (SMS, MMS y llamadas telefónicas) en archivos de registro de BlackBerry UEM. Durante la activación los usuarios deberán conceder los permisos de administrador a BlackBerry UEM Client.
Solo espacio de trabajo - (Samsung Knox)	Este tipo de activación permite administrar todo el dispositivo con comandos y reglas de políticas de TI de Knox MDM y Knox Workspace. Este tipo de activación elimina el espacio personal e instala un espacio de trabajo. El usuario debe crear una contraseña para acceder al dispositivo. Todos los datos del dispositivo estarán protegidos mediante cifrado y un método de autenticación, como una contraseña, un PIN, un patrón o una huella digital. Este tipo de activación es compatible con el registro de actividad del dispositivo (SMS, MMS y llamadas telefónicas) en archivos de registro de BlackBerry UEM. Durante la activación los usuarios deberán conceder los permisos de administrador a BlackBerry UEM Client.

Creación de perfiles de activación

Puede controlar el modo en que los dispositivos se activan y se gestionan mediante perfiles de activación. Un perfil de activación especifica cuántos y qué tipos de dispositivos puede activar un usuario y el tipo de activación para cada tipo de dispositivo.

El tipo de activación le permite configurar el nivel de control que tiene sobre los dispositivos activados. Es posible que desee tener el control total sobre un dispositivo que entrega a un usuario. Es posible que deba asegurarse de no tener ningún control sobre los datos personales en un dispositivo que un usuario posee y que lleva al trabajo.

El perfil de activación asignado se aplica solo a los dispositivos que el usuario activa después de que se asigne el perfil. Los dispositivos que ya están activados no se actualizan automáticamente para que coincida con el perfil de activación nuevo o actualizado.

Cuando se agrega un usuario a BlackBerry UEM, el perfil de activación predeterminado se asigna a la cuenta de usuario. Puede cambiar el perfil de activación predeterminado para satisfacer sus necesidades, o puede crear un perfil de activación personalizado y asignarlo a los usuarios o a los grupos de usuarios.

Creación de un perfil de activación

1. En la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Política > Activación**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil.
5. En el campo **Número de dispositivos que un usuario puede activar**, especifique el número máximo de dispositivos que el usuario puede activar.

6. En la lista desplegable **Propiedad del dispositivo**, seleccione la configuración predeterminada para la propiedad del dispositivo.
   - Seleccione **No especificado** en el caso de que algunos usuarios activen dispositivos personales y otros activen los dispositivos de trabajo.
   - Seleccione **Trabajo** si la mayoría de los usuarios activan los dispositivos de trabajo.
   - Seleccione **Personal** si los usuarios en su mayoría activan dispositivos personales.
7. Opcionalmente, seleccione un aviso de la empresa en la lista desplegable **Asignar aviso de la organización**. Si asigna un aviso de la empresa, los usuarios que activen los dispositivos con iOS, iPadOS, macOS o Windows 10 deberán aceptar el aviso para completar el proceso de activación.
8. En la sección **Tipos de dispositivo que los usuarios pueden activar**, seleccione los tipos de SO del dispositivo según sea necesario. Los tipos de dispositivo que no seleccione no se incluirán en el perfil de activación y los usuarios no podrán activar dichos dispositivos.
9. Realice las siguientes acciones para cada tipo de dispositivo incluido en el perfil de activación:
   a) Haga clic en la pestaña del tipo de dispositivo.
   b) En la lista desplegable **Restricciones de modelo de dispositivo**, seleccione una de las opciones siguientes:
      - **Sin restricciones**: los usuarios pueden activar cualquier modelo de dispositivo.
      - **Permitir modelos de dispositivo seleccionados**: los usuarios solo pueden activar los modelos de dispositivo que especifique. Utilice esta opción para limitar los dispositivos permitidos a solo algunos modelos.
      - **No permitir modelos de dispositivo seleccionados**: los usuarios no pueden activar los modelos de dispositivo especificados. Utilice esta opción para bloquear la activación de algunos modelos de dispositivo o dispositivos de fabricantes específicos.

      Si restringe los modelos de dispositivo que los usuarios pueden activar, haga clic en **Editar** para seleccionar los dispositivos que desea permitir o restringir y haga clic en **Guardar**.
   c) En la lista desplegable **Versión mínima permitida**, seleccione la versión mínima de SO permitida.

      Muchas versiones anteriores del SO ya no son compatibles con BlackBerry UEM. Solo debe seleccionar una versión mínima si no desea que sea compatible con la versión más antigua actualmente admitida por BlackBerry UEM. Para obtener más información sobre las versiones compatibles, consulte la Matriz de compatibilidad.
   d) Seleccione los tipos de activación compatibles.

      En el caso de dispositivos con Android, puede seleccionar varios tipos de activación y clasificarlos. Para el resto de tipos de dispositivos, solo podrá seleccionar un tipo de activación.

      El tipo de activación "Controles de MDM" está obsoleto en los dispositivos con Android 10 y posteriores. Se incluye en la lista de tipos de activación solo si la opción **Activar el tipo de activación de controles MDM para dispositivos Android** está seleccionada en la configuración de activación predeterminada.
10. Para dispositivos con Android, lleve a cabo las acciones siguientes:
   a) Si ha seleccionado más de un tipo de activación, haga clic en las flechas hacia arriba y hacia abajo para clasificarlas.

      Los dispositivos recibirán el perfil de mayor clasificación con el cual sean compatibles. Por ejemplo, si clasifica en primer lugar "Controles de MDM", los dispositivos que no admitan "Controles de MDM" recibirán el siguiente tipo de activación clasificado.
   b) Si ha seleccionado el tipo de activación "Controles de MDM" y no desea que se apliquen las reglas de políticas de MDM de Knox a los dispositivos con las cuales son compatibles, desmarque la casilla de verificación **Activar API de Samsung KNOX en activaciones de Controles de MDM**.
   c) Si ha seleccionado el tipo de activación Samsung Knox y desea utilizar Google Play para administrar las aplicaciones de trabajo, seleccione **Gestión de aplicaciones de Google Play para dispositivos Samsung Knox Workspace**. Esta opción está disponible únicamente si ha configurado una conexión a un dominio de Google.

Los tipos de activación Samsung Knox quedarán en desuso en una versión futura. Los dispositivos compatibles con Knox Platform for Enterprise se pueden activar mediante los tipos de activación Android Enterprise. Para obtener más información, visite https://support.blackberry.com/community para leer el artículo 54614.

d) Si ha seleccionado un tipo de activación Android Enterprise, marque las opciones de Android Enterprise correspondientes:
   - La opción **Al activar dispositivos Android Enterprise, active las funciones premium de UEM como BlackBerry Secure Connect Plus** activará las funciones de BlackBerry Secure Connect Plus y Knox Platform para Enterprise (para dispositivos que admiten Samsung Knox) en dispositivos con una licencia adecuada.
   - La opción **Activar Samsung Knox DualDAR Workspace** permite el cifrado de Samsung Knox DualDAR para dispositivos que sean compatibles con esta función. Esta opción solo es compatible con los dispositivos con "Solo espacio de trabajo" y " Trabajo y personal: control total".
   - La opción **Agregar cuenta de Google Play al espacio de trabajo** admite la gestión de aplicaciones de Google Play en el espacio de trabajo. Si el dispositivo no tiene acceso a Google Play, desmarque esta opción.
   - La opción **Permitir solo ID de dispositivo aprobados** le permite restringir la activación a dispositivos individuales para los que especifique el ID de dispositivo. Esta opción solo es compatible con los dispositivos con "Solo espacio de trabajo" y " Trabajo y personal: control total".
e) En la sección **Opciones de atestación de SafetyNet**, seleccione de forma opcional uno de los siguientes métodos de atestación:
   - **Realizar la atestación de SafetyNet para el dispositivo**: use este método para enviar comprobaciones para probar la autenticidad y la integridad de los dispositivos.
   - **Realizar la atestación de SafetyNet en la activación del dispositivo**: use este método para enviar comprobaciones para probar la autenticidad y la integridad de los dispositivos cuando están activados.
   - **Realizar la atestación de SafetyNet en la activación de la aplicación de BlackBerry Dynamics**: use este método para enviar comprobaciones para probar la autenticidad y la integridad de las aplicaciones de BlackBerry Dynamics cuando están activadas.
f) En la sección **Opciones de atestación de hardware**, seleccione **Aplicar reglas de cumplimiento de atestación durante la activación** si desea que BlackBerry UEM envíe comprobaciones a los dispositivos cuando están activados para garantizar que el nivel de revisión de seguridad necesario esté instalado.

11. Haga clic en **Agregar**.

Después de terminar: Si fuera necesario, clasifique los perfiles.

Activación de un dispositivo Android Enterprise con el tipo de activación de Trabajo y personal: privacidad de usuario

Estos pasos se aplican para la activación de dispositivos que tienen asignado el tipo de activación Trabajo y personal: privacidad de usuario (Android Enterprise). Los dispositivos con este tipo de activación no requieren que se restablezcan los valores predeterminados de fábrica para su activación.

Envíe las siguientes instrucciones de activación a los usuarios de dispositivos o envíeles un enlace al siguiente flujo de trabajo: Activación de su dispositivo Android.

Antes de empezar: El administrador de dispositivos le ha enviado uno o varios correos con la información que necesita para activar su dispositivo. Si el mensaje de correo electrónico incluye un QR Code de activación, puede utilizarlo para activar su dispositivo, así no tendrá que escribir información alguna. Si no ha recibido un QR Code, asegúrese de haber recibido la siguiente información:

- Dirección de correo electrónico del trabajo

- Nombre de usuario de BlackBerry UEM (normalmente el nombre de usuario del trabajo)
- Contraseña de activación de BlackBerry UEM
- Dirección del servidor de BlackBerry UEM (si es necesario)

1. Instale BlackBerry UEM Client en el dispositivo desde Google Play.

   Si el dispositivo no tiene acceso a Google Play, puede descargar UEM Client manualmente de BlackBerry e instalarlo. Para descargar el archivo .apk de la versión más reciente de UEM Client, visite support.blackberry.com/community y lea el artículo 42607.
2. Abra UEM Client.
3. Lea el acuerdo de licencia y toque la casilla de verificación **Acepto el acuerdo de licencia**.
4. Lleve a cabo una de estas acciones:

Tarea	Pasos
Utilice un QR Code para activar el dispositivo	**a.** Toque . **b.** Toque **Permitir** para permitir que UEM Client haga fotos y grabe vídeos. **c.** Escanee el QR Code del correo de activación que ha recibido.
Active manualmente el dispositivo	**a.** Escriba su dirección de correo electrónico de trabajo. Toque **Siguiente**. **b.** Escriba una contraseña de activación. Toque **Activar mi dispositivo**. **c.** Si es necesario, escriba la dirección del servidor. Puede encontrar la dirección del servidor en el mensaje de correo de activación que ha recibido o en BlackBerry UEM Self-Service. Toque **Siguiente**. **d.** Si es necesario, escriba su nombre de usuario y la contraseña de activación. Toque **Siguiente**.

5. Toque **Permitir** para que UEM Client realice y gestione llamadas telefónicas.
6. Espere mientras la configuración y los perfiles se cargan en el dispositivo.
7. En la pantalla **Configurar perfil**, toque **Configurar** y espere a que se configure el perfil de trabajo en el dispositivo.
8. Si se le solicita, inicie sesión en su cuenta de Google con su dirección de correo electrónico y su contraseña de Google.
9. En la pantalla de selección del método de desbloqueo, elija un método de desbloqueo de la pantalla.
10. Si se le solicita en la pantalla **Inicio seguro**, toque **Sí** para solicitar una contraseña cuando el dispositivo se inicie.
11. Escriba una contraseña del dispositivo y vuelva a escribirla para confirmarla. Toque **Aceptar**.
12. Seleccione una de las opciones para especificar cómo desea que se muestren las notificaciones. Toque **Hecho**.
13. Cree una contraseña para UEM Client y toque **Aceptar**. Si utiliza aplicaciones de BlackBerry Dynamics, también utilizará esta contraseña para iniciar sesión en todas sus aplicaciones de BlackBerry Dynamics.
14. En la siguiente pantalla, toque **Inscribirse** y siga las instrucciones que aparecen en pantalla si desea establecer una autenticación mediante huella dactilar para UEM Client o para cualquier aplicación de BlackBerry Dynamics que tenga. De lo contrario, toque **Cancelar**.
15. Si ha cerrado sesión en su dispositivo, desbloquéelo para completar la activación de BlackBerry UEM.
16. Si se le solicita, toque **Aceptar** para permitir la conexión con BlackBerry Secure Connect Plus y espere mientras la conexión esté activada.
17. Si se le solicita, siga las instrucciones que aparecen en pantalla para instalar las aplicaciones de trabajo en su dispositivo.

Después de terminar: Para verificar que el proceso de activación se ha completado correctamente, realice una de las siguientes acciones:

- En UEM Client, toque ⋮ > **Acerca de**. En la sección **Dispositivo activado**, compruebe que la información del dispositivo y la marca de tiempo de activación están presentes.
- En la consola de BlackBerry UEM Self-Service, compruebe que el dispositivo aparece como dispositivo activado. El estado puede tardar hasta dos minutos en actualizarse una vez que haya activado el dispositivo.

Activación de un dispositivo Android Enterprise cuando BlackBerry UEM se conecta a un dominio de Google

Estos pasos se aplican a los dispositivos que tienen asignado el tipo de activación Solo espacio de trabajo (Android Enterprise) o Trabajo y personal: control total (Android Enterprise) cuando BlackBerry UEM está conectado a un dominio de G Suite o Google Cloud. Para activar dispositivos que estén conectados a un dominio de Google con el tipo de activación Trabajo y personal: privacidad de usuario, consulte Activación de un dispositivo Android Enterprise con el tipo de activación de Trabajo y personal: privacidad de usuario.

En este tema se describe un método para activar dispositivos Android Enterprise. Para obtener información acerca de las opciones adicionales, consulte Activación de dispositivos con Android.

Envíe las instrucciones de activación siguientes al usuario del dispositivo.

Antes de empezar: El administrador de dispositivos le ha enviado uno o varios correos con la información que necesita para activar su dispositivo. Si el mensaje de correo electrónico incluye un QR Code de activación, puede utilizarlo para activar su dispositivo, así no tendrá que escribir información alguna. Si no ha recibido un QR Code, asegúrese de haber recibido la siguiente información:

- Dirección de correo electrónico del trabajo
- Nombre de usuario de activación de BlackBerry UEM (normalmente el nombre de usuario del trabajo)
- Contraseña de activación de BlackBerry UEM
- Dirección del servidor de BlackBerry UEM (si es necesario)

1. Si no ve la pantalla de bienvenida de configuración del dispositivo, restablezca el dispositivo con la configuración predeterminada de fábrica.
2. Durante la configuración de un dispositivo, en la pantalla de inicio de sesión de la cuenta de Google, introduzca su dirección de correo electrónico y contraseña de Google de trabajo.
3. En el dispositivo, toque **Instalar** para instalar BlackBerry UEM Client.
4. Lea el acuerdo de licencia y toque la casilla de verificación **Acepto el acuerdo de licencia**.
5. Lleve a cabo una de estas acciones:

Tarea	Pasos
Utilice un QR Code para activar el dispositivo	**a.** Toque . **b.** Toque **Permitir** para permitir que UEM Client haga fotos y grabe vídeos. **c.** Escanee el QR Code del correo de activación que ha recibido.
Active manualmente el dispositivo	**a.** Escriba su dirección de correo electrónico de trabajo. Toque **Siguiente**. **b.** Escriba una contraseña de activación. Toque **Activar mi dispositivo**. **c.** Si es necesario, escriba la dirección del servidor. Puede encontrar la dirección del servidor en el mensaje de correo de activación que ha recibido o en BlackBerry UEM Self-Service. Toque **Siguiente**.

Tarea	Pasos
	d. Si es necesario, escriba su nombre de usuario y la contraseña de activación. Toque **Siguiente**.

6. Espere mientras la configuración y los perfiles se cargan en el dispositivo.
7. En la pantalla **Configurar perfil**, toque **Configurar** y espere a que se configure el perfil de trabajo en el dispositivo.
8. Si se le solicita, inicie sesión en su cuenta de Google con su dirección de correo electrónico y su contraseña de Google.
9. En la pantalla de selección del método de desbloqueo, elija un método de desbloqueo de la pantalla.
10. Si se le solicita en la pantalla **Inicio seguro**, toque **Sí** para solicitar una contraseña cuando el dispositivo se inicie.
11. Escriba una contraseña del dispositivo y vuelva a escribirla para confirmarla. Toque **Aceptar**.
12. Seleccione una de las opciones para especificar cómo desea que se muestren las notificaciones. Toque **Hecho**.
13. Cree una contraseña para UEM Client y toque **Aceptar**. Si utiliza aplicaciones de BlackBerry Dynamics, también utilizará esta contraseña para iniciar sesión en todas sus aplicaciones de BlackBerry Dynamics.
14. En la siguiente pantalla, toque **Inscribirse** y siga las instrucciones que aparecen en pantalla si desea establecer una autenticación mediante huella dactilar para UEM Client o para cualquier aplicación de BlackBerry Dynamics que tenga. De lo contrario, toque **Cancelar**.
15. Si ha cerrado sesión en su dispositivo, desbloquéelo para completar la activación de BlackBerry UEM.
16. Si se le solicita, toque **Aceptar** para permitir la conexión con BlackBerry Secure Connect Plus y espere mientras la conexión esté activada.
17. Si se le solicita, siga las instrucciones que aparecen en pantalla para instalar las aplicaciones de trabajo en su dispositivo.

Después de terminar: Para verificar que el proceso de activación se ha completado correctamente, realice una de las siguientes acciones:

- En UEM Client, toque ⋮ > **Acerca de**. En la sección **Dispositivo activado**, compruebe que la información del dispositivo y la marca de tiempo de activación están presentes.
- En la consola de BlackBerry UEM Self-Service, compruebe que el dispositivo aparece como dispositivo activado. El estado puede tardar hasta dos minutos en actualizarse una vez que haya activado el dispositivo.

Activar un dispositivo Android Enterprise con el tipo de activación Solo espacio de trabajo mediante una cuenta de Google Play gestionada

En este tema se describe un método para activar dispositivos Android Enterprise. Para obtener información acerca de las opciones adicionales, consulte Activación de dispositivos con Android.

Estas instrucciones también son aplicables a dispositivos con Android 10 con el tipo de activación Trabajo y personal: control total.

Para dispositivos con Android 8 y 9, consulte Activar un dispositivo Android Enterprise con el tipo de activación Trabajo y personal: control total mediante una cuenta de Google Play gestionada en su lugar. Los dispositivos con Android 8 y 9 ya no admiten el hashtag afw#blackberry para iniciar activaciones Solo espacio de trabajo o Trabajo y personal: control total.

Envíe las instrucciones de activación siguientes al usuario del dispositivo.

Antes de empezar: El administrador de dispositivos le ha enviado uno o varios correos con la información que necesita para activar su dispositivo. Si el administrador le ha enviado un QR Code de activación, puede utilizarlo para activar su dispositivo sin necesidad de escribir ninguna información. Si no ha recibido un QR Code, asegúrese de haber recibido la siguiente información:

- Dirección de correo electrónico del trabajo
- Nombre de usuario de activación de BlackBerry UEM (normalmente el nombre de usuario del trabajo)
- Contraseña de activación de BlackBerry UEM
- Dirección del servidor de BlackBerry UEM (si es necesario)

1. Si no ve la pantalla de bienvenida de configuración del dispositivo, restablezca el dispositivo con la configuración predeterminada de fábrica.
2. Durante la configuración del dispositivo, escriba afw#blackberry en la pantalla de inicio de sesión de la cuenta de Google.
3. Toque **Instalar** para instalar BlackBerry UEM Client.
4. Lea el acuerdo de licencia y toque la casilla de verificación **Acepto el acuerdo de licencia**.
5. Lleve a cabo una de estas acciones:

Tarea	Pasos
Utilice un QR Code para activar el dispositivo	**a.** Toque . **b.** Toque **Permitir** para permitir que UEM Client haga fotos y grabe vídeos. **c.** Escanee el QR Code del correo de activación que ha recibido.
Active manualmente el dispositivo	**a.** Escriba su dirección de correo electrónico de trabajo. Toque **Siguiente**. **b.** Escriba una contraseña de activación. Toque **Activar mi dispositivo**. **c.** Si es necesario, escriba la dirección del servidor. Puede encontrar la dirección del servidor en el mensaje de correo de activación que ha recibido o en BlackBerry UEM Self-Service. Toque **Siguiente**. **d.** Si es necesario, escriba su nombre de usuario y la contraseña de activación. Toque **Siguiente**.

6. Espere mientras la configuración y los perfiles se cargan en el dispositivo.
7. En la pantalla **Configurar perfil**, toque **Configurar** y espere a que se configure el perfil de trabajo en el dispositivo.
8. Si se le solicita, inicie sesión en su cuenta de Google con su dirección de correo electrónico y su contraseña de Google.
9. En la pantalla de selección del método de desbloqueo, elija un método de desbloqueo de la pantalla.
10. Si se le solicita en la pantalla **Inicio seguro**, toque **Sí** para solicitar una contraseña cuando el dispositivo se inicie.
11. Escriba una contraseña del dispositivo y vuelva a escribirla para confirmarla. Toque **Aceptar**.
12. Seleccione una de las opciones para especificar cómo desea que se muestren las notificaciones. Toque **Hecho**.
13. Cree una contraseña para UEM Client y toque **Aceptar**. Si utiliza aplicaciones de BlackBerry Dynamics, también utilizará esta contraseña para iniciar sesión en todas sus aplicaciones de BlackBerry Dynamics.
14. En la siguiente pantalla, toque **Inscribirse** y siga las instrucciones que aparecen en pantalla si desea establecer una autenticación mediante huella dactilar para UEM Client o para cualquier aplicación de BlackBerry Dynamics que tenga. De lo contrario, toque **Cancelar**.
15. Si ha cerrado sesión en su dispositivo, desbloquéelo para completar la activación de BlackBerry UEM.

16. Si se le solicita, toque **Aceptar** para permitir la conexión con BlackBerry Secure Connect Plus y espere mientras la conexión esté activada.
17. Si se le solicita, siga las instrucciones que aparecen en pantalla para instalar las aplicaciones de trabajo en su dispositivo.

Después de terminar: Para verificar que el proceso de activación se ha completado correctamente, realice una de las siguientes acciones:

- En UEM Client, toque ⋮ > **Acerca de**. En la sección **Dispositivo activado**, compruebe que la información del dispositivo y la marca de tiempo de activación están presentes.
- En la consola de BlackBerry UEM Self-Service, compruebe que el dispositivo aparece como dispositivo activado. El estado puede tardar hasta dos minutos en actualizarse una vez que haya activado el dispositivo.

Activar un dispositivo Android Enterprise con el tipo de activación Trabajo y personal: control total mediante una cuenta de Google Play gestionada

En este tema se describe un método para activar dispositivos Android Enterprise. Para obtener información acerca de las opciones adicionales, consulte Activación de dispositivos con Android.

Para dispositivos con Android 10, las instrucciones para activar un dispositivo Android Enterprise con el tipo de activación Solo espacio de trabajo mediante una cuenta de Google Play gestionada también funcionan para el tipo de activación Trabajo y personal: control total. Android 11 ya no admite el uso del hashtag afw#blackberry para iniciar activaciones Trabajo y personal: control total.

Estas instrucciones utilizan el QR Code para indicar al dispositivo que descargue e instale BlackBerry UEM Client. Para permitir que los usuarios inicien la descarga con el QR Code, en la configuración de activación predeterminada, debe seleccionar **Permitir que el código QR contenga la ubicación del archivo de origen de la aplicación de UEM Client**. Para obtener más información, consulte Especificación de la configuración de activación predeterminada.

Envíe las instrucciones de activación siguientes al usuario del dispositivo.

Antes de empezar: El administrador de dispositivos le ha enviado uno o varios correos con la información que necesita para activar su dispositivo. El mensaje de correo electrónico incluye un QR Code con la información necesaria para instalar UEM Client y activar el dispositivo.

1. En el dispositivo en el que desee realizar la activación, si no ve la primera pantalla de configuración del dispositivo, restablezca la configuración predeterminada de fábrica del dispositivo.
2. Toque la pantalla del dispositivo siete veces.

   Se abrirá un lector de QR Code en el dispositivo.
3. Lea el acuerdo de licencia y toque la casilla de verificación **Acepto el acuerdo de licencia**.
4. Espere mientras la configuración y los perfiles se cargan en el dispositivo.
5. En la pantalla **Configurar perfil**, toque **Configurar** y espere a que se configure el perfil de trabajo en el dispositivo.
6. Si se le solicita, inicie sesión en su cuenta de Google con su dirección de correo electrónico y su contraseña de Google.
7. En la pantalla de selección del método de desbloqueo, elija un método de desbloqueo de la pantalla.
8. Si se le solicita en la pantalla **Inicio seguro**, toque **Sí** para solicitar una contraseña cuando el dispositivo se inicie.
9. Escriba una contraseña del dispositivo y vuelva a escribirla para confirmarla. Toque **Aceptar**.

10. Seleccione una de las opciones para especificar cómo desea que se muestren las notificaciones. Toque **Hecho**.
11. Cree una contraseña para UEM Client y toque **Aceptar**. Si utiliza aplicaciones de BlackBerry Dynamics, también utilizará esta contraseña para iniciar sesión en todas sus aplicaciones de BlackBerry Dynamics.
12. En la siguiente pantalla, toque **Inscribirse** y siga las instrucciones que aparecen en pantalla si desea establecer una autenticación mediante huella dactilar para UEM Client o para cualquier aplicación de BlackBerry Dynamics que tenga. De lo contrario, toque **Cancelar**.
13. Si ha cerrado sesión en su dispositivo, desbloquéelo para completar la activación de BlackBerry UEM.
14. Si se le solicita, toque **Aceptar** para permitir la conexión con BlackBerry Secure Connect Plus y espere mientras la conexión esté activada.
15. Si se le solicita, siga las instrucciones que aparecen en pantalla para instalar las aplicaciones de trabajo en su dispositivo.

Después de terminar: Para verificar que el proceso de activación se ha completado correctamente, realice una de las siguientes acciones:

- En UEM Client, toque ⋮ > **Acerca de**. En la sección **Dispositivo activado**, compruebe que la información del dispositivo y la marca de tiempo de activación están presentes.
- En la consola de BlackBerry UEM Self-Service, compruebe que el dispositivo aparece como dispositivo activado. El estado puede tardar hasta dos minutos en actualizarse una vez que haya activado el dispositivo.

Activación de un dispositivo Android Enterprise sin acceso a Google Play

Estos pasos sirven para activar dispositivos Android que no tienen acceso a Google Play con los tipos de activación Solo espacio de trabajo (Android Enterprise) y Trabajo y personal: control total (Android Enterprise). Para activar dispositivos con el tipo de activación Trabajo y personal: privacidad de usuario (Android Enterprise), consulte: Activación de un dispositivo Android Enterprise con el tipo de activación de Trabajo y personal: privacidad de usuario.

Para iniciar la activación, el dispositivo debe estar configurado con los ajustes predeterminados de fábrica y recibir las instrucciones para descargar BlackBerry UEM Client mediante QR Code o NFC.

- Puede incluir la ubicación de descarga de UEM Client en el código QR que reciben los usuarios en el correo electrónico de activación. Los usuarios pueden escanear QR Code para iniciar la descarga. Para obtener más información, consulte Configuración predeterminada de activación de dispositivos.
- Puede preprogramar un adhesivo NFC que los usuarios pueden tocar para iniciar la activación del dispositivo.
- En los dispositivos Android 9 y anteriores, los usuarios pueden utilizar NFC y tocar un dispositivo secundario que tenga instalada la aplicación BlackBerry UEM Enroll. Para descargar e instalar la aplicación UEM Enroll en un dispositivo secundario, visite support.blackberry.com/community para leer el artículo 42607.

Se puede utilizar el mismo dispositivo secundario o adhesivo NFC para activar dispositivos para varios usuarios.

Si desea que el usuario inicie la activación del dispositivo mediante QR Code, envíe las instrucciones de activación para Activar un dispositivo Android Enterprise con el tipo de activación Trabajo y personal: control total mediante una cuenta de Google Play gestionada al usuario del dispositivo.

Si desea que los usuarios inicien la activación del dispositivo mediante NFC, envíe las siguientes instrucciones de activación al usuario del dispositivo:

Antes de empezar:

- El administrador de dispositivos le ha enviado uno o varios correos con la información que necesita para activar su dispositivo. Si el administrador le ha enviado un QR Code de activación, puede utilizarlo para activar

su dispositivo sin necesidad de escribir ninguna información. Si no ha recibido un QR Code, asegúrese de haber recibido la siguiente información:
  - Dirección de correo electrónico del trabajo
  - Nombre de usuario de activación de BlackBerry UEM (normalmente el nombre de usuario del trabajo)
  - Contraseña de activación de BlackBerry UEM
  - Dirección del servidor de BlackBerry UEM (si es necesario)
- El administrador le proporcionará un adhesivo NFC preprogramado o un dispositivo secundario que tenga instalada la aplicación UEM Enroll.

1. En el dispositivo en el que desee realizar la activación, si no ve la pantalla de bienvenida de configuración del dispositivo, restablezca el dispositivo con la configuración predeterminada de fábrica.
2. Lleve a cabo una de estas acciones:

Tarea	Pasos
Inicie la activación con un adhesivo NFC	**a.** Toque el dispositivo con el adhesivo NFC proporcionada por el administrador. El dispositivo descarga e instala UEM Client. **b.** Siga las indicaciones cuando el dispositivo se prepare para la activación.
Inicie la activación con un dispositivo secundario	**a.** En el dispositivo secundario, abra la aplicación UEM Enroll. Asegúrese de tener NFC habilitado en el dispositivo. **b.** Toque **Activar dispositivo**. **c.** Junte la parte posterior de dos dispositivos. Cuando se le solicite, toque en cualquier parte de la pantalla del dispositivo secundario. **d.** En el dispositivo en el que desee realizar la activación, siga las instrucciones que aparecen en la pantalla e instale UEM Client.

3. Lea el acuerdo de licencia y toque la casilla de verificación **Acepto el acuerdo de licencia**.
4. Lleve a cabo una de estas acciones:

Tarea	Pasos
Utilice un QR Code para activar el dispositivo	**a.** Toque . **b.** Toque **Permitir** para permitir que UEM Client haga fotos y grabe vídeos. **c.** Escanee el QR Code del correo de activación que ha recibido.
Active manualmente el dispositivo	**a.** Escriba su dirección de correo electrónico de trabajo. Toque **Siguiente**. **b.** Escriba una contraseña de activación. Toque **Activar mi dispositivo**. **c.** Si es necesario, escriba la dirección del servidor. Puede encontrar la dirección del servidor en el mensaje de correo de activación que ha recibido o en BlackBerry UEM Self-Service. Toque **Siguiente**. **d.** Si es necesario, escriba su nombre de usuario y la contraseña de activación. Toque **Siguiente**.

5. Espere mientras la configuración y los perfiles se cargan en el dispositivo.
6. En la pantalla **Configurar perfil**, toque **Configurar** y espere a que se configure el perfil de trabajo en el dispositivo.
7. En la pantalla de selección del método de desbloqueo, elija un método de desbloqueo de la pantalla.
8. Si se le solicita en la pantalla **Inicio seguro**, toque **Sí** para solicitar una contraseña cuando el dispositivo se inicie.
9. Escriba una contraseña del dispositivo y vuelva a escribirla para confirmarla. Toque **Aceptar**.

10. Seleccione una de las opciones para especificar cómo desea que se muestren las notificaciones. Toque **Hecho**.
11. Cree una contraseña para UEM Client y toque **ACEPTAR**. Si utiliza aplicaciones de BlackBerry Dynamics, también utilizará esta contraseña para iniciar sesión en todas sus aplicaciones de BlackBerry Dynamics.
12. En la siguiente pantalla, toque **Inscribirse** y siga las instrucciones que aparecen en pantalla si desea establecer una autenticación mediante huella dactilar para UEM Client o para cualquier aplicación de BlackBerry Dynamics que tenga. De lo contrario, toque **Cancelar**.
13. Si ha cerrado sesión en su dispositivo, desbloquéelo para completar la activación de BlackBerry UEM.
14. Si se le solicita, toque **Aceptar** para permitir la conexión con BlackBerry Secure Connect Plus y espere mientras la conexión esté activada.
15. Si se le solicita, siga las instrucciones que aparecen en pantalla para instalar las aplicaciones de trabajo en su dispositivo.
16. Si fuera necesario, abra la aplicación de correo electrónico que su empresa desea que utilice (por ejemplo,) y siga las instrucciones para configurar el correo electrónico en su teléfono.

Activación de un dispositivo Android con el tipo de activación de Controles de MDM

Nota: Estos pasos solo se aplican a dispositivos asignados al tipo de activación de Controles de MDM. Este tipo de activación está obsoleta en Android 10. Los intentos de activar dispositivos con Android 10 y versiones posteriores con el tipo de activación de Controles de MDM fallarán. Para obtener más información, https://support.blackberry.com/community para leer el artículo 48386.

Envíe las instrucciones de activación siguientes al usuario del dispositivo.

1. Instale BlackBerry UEM Client en el dispositivo desde Google Play.
2. Abra UEM Client.
3. Lea el acuerdo de licencia y toque la casilla de verificación **Acepto el acuerdo de licencia**.
4. Lleve a cabo una de estas acciones:

Tarea	Pasos
Utilice un QR Code para activar el dispositivo	a. Toque . b. Toque **Permitir** para permitir que UEM Client haga fotos y grabe vídeos. c. Escanee el QR Code del correo de activación que ha recibido.
Active manualmente el dispositivo	a. Escriba su dirección de correo electrónico de trabajo. Toque **Siguiente**. b. Escriba una contraseña de activación. Toque **Activar mi dispositivo**. c. Si es necesario, escriba la dirección del servidor. Puede encontrar la dirección del servidor en el mensaje de correo de activación que ha recibido o en BlackBerry UEM Self-Service. Toque **Siguiente**. d. Si es necesario, escriba su nombre de usuario y la contraseña de activación. Toque **Siguiente**.

5. Toque **Siguiente**.
6. Toque **Activar** para activar el administrador de dispositivos. Debe activar el administrador del dispositivo para poder acceder a los datos de trabajo en el dispositivo.
7. Si se le solicita, toque **Aceptar** para permitir la conexión con BlackBerry Secure Connect Plus y espere mientras la conexión esté activada.

8. Si se le solicita, siga las instrucciones que aparecen en pantalla para instalar las aplicaciones de trabajo en su dispositivo.

Después de terminar: Para verificar que el proceso de activación se ha completado correctamente, realice una de las siguientes acciones:

- En UEM Client, toque ⋮ > **Acerca de**. En la sección **Dispositivo activado**, compruebe que la información del dispositivo y la marca de tiempo de activación están presentes.
- En la consola de BlackBerry UEM Self-Service, compruebe que el dispositivo aparece como dispositivo activado. El estado puede tardar hasta dos minutos en actualizarse una vez que haya activado el dispositivo.

Administración y control de dispositivos Android activados

Cuando los dispositivos se activen y administren por medio de una política de TI y perfiles, tendrá varias funciones disponibles para controlar los dispositivos de los usuarios.

Tiene las siguientes opciones:

Opción	Descripción
Controlar las actualizaciones de software que se instalan en los dispositivos y las fechas de las actualizaciones.	Puede utilizar un perfil de requisitos de informe especial del dispositivo cuando se instalen actualizaciones del SO en los siguientes operativos: • Dispositivos Android Enterprise con la activación Solo espacio de trabajo • Dispositivos con Samsung Knox Para obtener más información, consulte el contenido de Administración. Puede utilizar los perfiles de conformidad para especificar versiones de SO restringidas. Para obtener más información, consulte el contenido de Administración.
Activar la configuración de ubicación y localizar un dispositivo	Puede activar la configuración de ubicación para realizar un seguimiento de la ubicación de los dispositivos Android. Para obtener más información, consulte el contenido de Administración.
Recuperación de registros del dispositivo	Puede recuperar registros de dispositivos para fines de control y resolución de problemas. Para obtener más información, consulte el contenido de Administración.
Desactivar un dispositivo	Cuando usted o un usuario desactiva el dispositivo, la conexión entre el dispositivo y la cuenta de usuario en BlackBerry UEM se elimina. No se puede gestionar el dispositivo y ya no aparece en la consola de gestión. El usuario no puede acceder a los datos de trabajo en el dispositivo. Puede desactivar un dispositivo mediante los comandos "Eliminar todos los datos del dispositivo" o "Eliminar solo los datos de trabajo". Los usuarios pueden desactivar un dispositivo Android mediante la selección de la opción Desactivar mi dispositivo en la pantalla Acerca de la aplicación BlackBerry UEM Client.

Comandos para dispositivos Android

Comando	Descripción	Tipos de activación
Ver informe del dispositivo	Este comando muestra información detallada acerca de un dispositivo. Puede exportar y guardar el informe del dispositivo en el equipo. Para obtener más información, consulte Ver y guardar un informe de dispositivo.	Todos (excepto BlackBerry 2FA)
Ver acciones de dispositivo	Este comando muestra todas las acciones que están en curso en un dispositivo. Para obtener más información, consulte Ver acciones de dispositivo.	Todos (excepto BlackBerry 2FA)
Bloquear dispositivo	Este comando bloquea el dispositivo. El usuario debe escribir la contraseña del dispositivo para desbloquear el dispositivo. Si un dispositivo se pierde de manera temporal, puede utilizar este comando. Cuando se envía este comando, el dispositivo se bloquea solo si existe una contraseña para el dispositivo. De lo contrario, no se realiza ninguna acción en el dispositivo.	Controles de MDM Trabajo y personal: control total (Android Enterprise) Trabajo y personal: privacidad de usuario (Android Enterprise) Solo espacio de trabajo (Android Enterprise)
Eliminar todos los datos del dispositivo	Este comando elimina toda la información del usuario y los datos de aplicaciones que almacena el dispositivo, incluida la información en el espacio de trabajo, y devuelve el dispositivo a la configuración predeterminada de fábrica. Si el dispositivo no se puede conectar a BlackBerry UEM cuando envía este comando, puede cancelar el comando o eliminar el dispositivo de la consola. Si el dispositivo se conecta a BlackBerry UEM una vez que lo elimine, solo se eliminarán los datos de trabajo del dispositivo, incluido el espacio de trabajo, si procede. Para enviar este comando a varios dispositivos, consulte Envío de un comando masivo.	Controles de MDM Trabajo y personal: control total (Android Enterprise) Trabajo y personal: control total (Samsung Knox) Solo espacio de trabajo - (Samsung Knox)

Comando	Descripción	Tipos de activación
Eliminar solo los datos de trabajo	Este comando elimina datos de trabajo, incluida la política de TI, los perfiles, aplicaciones y certificados que se encuentran en el dispositivo y desactiva el dispositivo. Si el dispositivo tiene un espacio de trabajo, la información del espacio de trabajo y el espacio de trabajo se eliminarán del dispositivo, pero todas las aplicaciones y datos personales permanecerán en el dispositivo. Para obtener más información, consulte Desactivación de dispositivos. Cuando utiliza este comando en dispositivos con Android Enterprise, puede escribir un motivo para que aparezca en la notificación del dispositivo del usuario para explicar por qué se borró el perfil de trabajo. Para activaciones Trabajo y personal: control total (Android Enterprise), este comando solo es compatible con dispositivos que ejecuten Android 11 y posterior. Si el dispositivo no se puede conectar a BlackBerry UEM cuando envía este comando, puede cancelar el comando o eliminar el dispositivo de la consola. Si el dispositivo se conecta a BlackBerry UEM una vez que lo haya eliminado, se eliminarán los datos de trabajo del dispositivo, incluido el espacio de trabajo, si procede. Para enviar este comando a varios dispositivos, consulte Envío de un comando masivo.	Controles de MDM Trabajo y personal: privacidad de usuario (Android Enterprise) Trabajo y personal: control total (Android Enterprise) Trabajo y personal: privacidad de usuario (Samsung Knox) Trabajo y personal: control total (Samsung Knox) Solo espacio de trabajo - (Samsung Knox)
Desbloquear dispositivo y borrar contraseña	Este comando desbloquea el dispositivo y solicita al usuario que cree una nueva contraseña para el dispositivo. Si el usuario omite la pantalla "Crear contraseña de dispositivo" se conserva la contraseña anterior. Puede utilizar este comando si un usuario olvida la contraseña del dispositivo. **Nota:** Este comando no es compatible con dispositivos con Samsung Knox SDK 3.2.1 y posterior.	Controles de MDM (solo dispositivos Samsung) Trabajo y personal: control total (Samsung Knox) Trabajo y personal: privacidad de usuario (Samsung Knox)
Especificar la contraseña del dispositivo y bloquearlo	Este comando permite crear una contraseña del dispositivo y, a continuación, bloquear el dispositivo. Debe crear una contraseña que cumpla con las actuales reglas para la contraseña. Para desbloquear el dispositivo, el usuario debe escribir la nueva contraseña. **Nota:** Para los tipos de activación Trabajo y personal: privacidad de usuario, solo los dispositivos BlackBerry con Android 8.x y posteriores son compatibles con este comando. **Nota:** Para el tipo de activación Trabajo y personal: control total (Android Enterprise), solo los dispositivos que utilizan una versión del sistema operativo Android anterior a Android 11 admiten este comando.	Trabajo y personal: control total (Samsung Knox) Solo espacio de trabajo (Android Enterprise) Trabajo y personal: control total (Android Enterprise) Trabajo y personal: privacidad de usuario (Android Enterprise)

Comando	Descripción	Tipos de activación
Restablecer contraseña del espacio de trabajo	Este comando elimina la contraseña actual del espacio de trabajo del dispositivo. Cuando el usuario abre el espacio de trabajo, el dispositivo solicita al usuario que defina una nueva contraseña del espacio de trabajo.	Trabajo y personal: control total (Samsung Knox) Trabajo y personal: privacidad de usuario - (Samsung Knox) Solo espacio de trabajo - (Samsung Knox)
Especificar contraseña de espacio de trabajo y bloquear	Puede especificar una contraseña para el perfil de trabajo y bloquear el dispositivo. Cuando el usuario abre una aplicación de trabajo, debe introducir la contraseña que se especificó.	Trabajo y personal: privacidad de usuario (Android Enterprise) Trabajo y personal: control total (Android Enterprise)
Desactivar/ activar espacio de trabajo	Este comando desactiva o activa el acceso a las aplicaciones del espacio de trabajo en el dispositivo.	Trabajo y personal: control total (Samsung Knox) Trabajo y personal: privacidad de usuario - (Samsung Knox) Solo espacio de trabajo - (Samsung Knox)
Desactivar BlackBerry 2FA	Este comando desactiva los dispositivos que se activan con el tipo de activación BlackBerry 2FA. El dispositivo se elimina de BlackBerry UEM y el usuario no puede utilizar la característica BlackBerry 2FA.	BlackBerry 2FA
Limpiar aplicaciones	Este comando borra los datos de todas las aplicaciones gestionadas por Microsoft Intune en el dispositivo. Las aplicaciones no se eliminan del dispositivo. Para obtener más información, consulte Borrar aplicaciones gestionadas por Microsoft Intune.	Todas (excepto BlackBerry 2FA)
Actualizar la información del dispositivo	Este comando envía y recibe información del dispositivo actualizada. Por ejemplo, puede enviar reglas de políticas de TI actualizadas recientemente o perfiles a un dispositivo y recibir información actualizada acerca de un dispositivo, como la versión del SO o el nivel de la batería. Para enviar este comando a varios dispositivos, consulte Envío de un comando masivo.	Todos (excepto BlackBerry 2FA)
Solicitar informe de errores	Este comando envía una solicitud al dispositivo para los registros de cliente. El usuario de dispositivo debe aceptar o rechazar la solicitud.	Solo espacio de trabajo (Android Enterprise) Trabajo y personal: control total (Android Enterprise)

Comando	Descripción	Tipos de activación
Reiniciar dispositivo	Este comando envía una solicitud al dispositivo para que se reinicie. En un mensaje se indica al usuario que el dispositivo se reiniciará en un minuto. El usuario de dispositivo tiene la opción de retrasar 10 minutos el reinicio.	Solo espacio de trabajo (Android Enterprise)
Eliminar dispositivo	Este comando elimina el dispositivo de BlackBerry UEM, pero no borra los datos del dispositivo. El dispositivo puede seguir recibiendo correos electrónicos y otros datos de trabajo. Este comando está destinado para los dispositivos que se hayan dañado o perdido de forma irreversible y no se espere que vuelvan a contactar con el servidor. Si un dispositivo que se haya eliminado intenta contactar con BlackBerry UEM, el usuario recibe una notificación y el dispositivo no podrá comunicarse con BlackBerry UEM a menos que se reactive. Para enviar este comando a varios dispositivos, consulte Envío de un comando masivo.	Todos (excepto BlackBerry 2FA)

Aviso legal

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

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

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

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

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

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

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

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

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

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

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

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

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

Publicado en Canadá