BlackBerry UEM

Activación de dispositivos

12.20

Contents

Activación de dispositivos con BlackBerry UEM

Cuando usted o un usuario activan un dispositivo, este se asocia con BlackBerry UEM. Esto le permite administrar y asignar configuraciones a los dispositivos, y proporciona a los usuarios acceso a los datos de trabajo en sus dispositivos.

Al activar un dispositivo, puede enviar los perfiles y las políticas de TI para controlar y configurar las características y administrar la seguridad de los datos de trabajo. También puede asignar aplicaciones para que el usuario las instale. En función del nivel de control que el tipo de activación seleccionado permita, también podrá proteger el dispositivo mediante la restricción del acceso a determinados datos, la configuración de contraseñas de forma remota, el bloqueo del dispositivo o la eliminación de datos.

Puede asignar distintos tipos de activación para adaptarse a los requisitos de los dispositivos que son propiedad de la empresa y los dispositivos que son propiedad de los usuarios. Los distintos tipos de activación le ofrecen distintos grados de control sobre los datos de trabajo y los datos personales en los dispositivos, que van desde el total control sobre todos los datos al control específico únicamente de los datos de trabajo.

Para configurar UEM para permitir que los usuarios activen dispositivos, debe realizar las siguientes acciones:

Paso	Acción
1	Compruebe que haya una licencia UEM disponible para cada dispositivo que desee activar. Para los dispositivos iOS iPadOS Android,compruebe que esté instalada la versión más reciente de BlackBerry UEM Client en el dispositivo desde la tienda de aplicaciones correspondiente.
2	Ajuste de la configuración de activación predeterminada.
3	Revise la información relevante para su entorno UEM y los usuarios de dispositivos: • Compatibilidad de las activaciones de Android Enterprise y Android Management • Ayuda con las activaciones de Windows 10 • Compatibilidad de la inscripción de usuario de Apple para dispositivos con iOS y iPadOS • Compatibilidad con Samsung Knox DualDAR • Configuración de la compatibilidad con el aprovisionamiento automático de Android • Active varios dispositivos mediante Knox Mobile Enrollment • Activación de los dispositivos iOS que están inscritos en DEP • Activación de dispositivos iOS mediante Apple Configurator 2
4	Actualice la plantilla para el correo de activación.
5	Cree un perfil de activación y asígnelo a cuentas de usuario o a grupos de usuarios.
6	Envío de un mensaje de correo electrónico de activación a varios usuarios, envíe un correo electrónico de activación a un usuario específico o permita que los usuarios establezcan su propia contraseña de activación en UEM Self-Service.

Paso	Acción
7	Envíe instrucciones de activación a los usuarios: • Activación de dispositivos Android • Activación de dispositivos iOS • Activación de un dispositivo con macOS o Apple TV con BlackBerry UEM Self-Service • Activación de una tableta o un equipo Windows 10

Tipos de activación: dispositivos iOS

Tipo de activación	Descripción
Controles de MDM	Este tipo de activación proporciona una gestión de dispositivos básica mediante controles de dispositivos puestos a disposición por dispositivos iOS y iPadOS. No se instala un espacio de trabajo separado en el dispositivo y no hay seguridad adicional para los datos de trabajo. Puede controlar el dispositivo a través de comandos y políticas de TI. Durante la activación, los usuarios deben instalar un perfil de gestión de dispositivos móviles en el dispositivo. Para especificar si BlackBerry UEM puede limitar la activación por ID de dispositivo, seleccione "Permitir solo ID de dispositivo aprobados".

Tipo de activación	Descripción
Privacidad del usuario	Este tipo de activación proporciona un control básico de los dispositivos a la vez que garantiza la privacidad de los datos personales de los usuarios. No se instala un contenedor independiente en el dispositivo y no se proporciona seguridad adicional para los datos de trabajo. Los dispositivos pueden utilizar servicios como Find my Phone y Root Detection, pero los administradores no pueden controlar las políticas de los dispositivos. **Nota:** Para licencias basadas en SIM, debe seleccionar "Permitir el acceso a la tarjeta SIM y a la información del hardware del dispositivo para activar licencias basadas en SIM" en el perfil de activación. Los usuarios deben instalar un perfil de MDM que solo pueda tener acceso a la tarjeta SIM y a la información del hardware del dispositivo que se necesita para comprobar si una licencia apropiada de SIM está disponible (por ejemplo, ICCID e IMEI). Los dispositivos Apple TV no admiten este tipo de activación. Cuando permita activaciones Privacidad del usuario, seleccione los perfiles que desea gestionar en el dispositivo en función de las necesidades de su empresa. Puede elegir cualquiera de las siguientes opciones: • Permitir el acceso a la tarjeta SIM y a la información del hardware del dispositivo para activar licencias basadas en SIM: esta opción especifica si UEM puede acceder a la tarjeta SIM y a la información del hardware del dispositivo, como el ICCID y el IMEI, para comprobar si hay disponible una licencia de SIM apropiada. • Permitir gestión de aplicaciones: esta opción especifica si desea instalar o eliminar aplicaciones de trabajo en el dispositivo y muestra una lista de las aplicaciones de trabajo instaladas en la pantalla de detalles del usuario. También puede especificar si se permiten accesos directos de aplicaciones. • Permitir administración de políticas de TI: esta opción especifica si desea aplicar un conjunto limitado de reglas de políticas de TI al dispositivo (políticas de contraseña, permitir capturas de pantalla, permitir documentos de fuentes gestionadas en destinos no gestionados y permitir documentos de fuentes no gestionadas en destinos gestionados). • Permitir administración de correo electrónico: esta opción especifica si se aplica al dispositivo la configuración del perfil de correo asignada al usuario. • Permitir administración de perfiles Wi-Fi: esta opción especifica si se aplica al dispositivo la configuración del perfil Wi-Fi asignada al usuario. • Permitir administración de VPN: esta opción especifica si se aplica al dispositivo la configuración de perfil VPN asignada al usuario.

Tipo de activación	Descripción
Privacidad de usuario: inscripción de usuario	Este tipo de activación puede utilizarse para dispositivos iOS y iPadOS para garantizar que los datos del usuario se mantengan privados y separados de los datos de trabajo. Se instala un espacio de trabajo independiente en el dispositivo para las aplicaciones de trabajo y las aplicaciones Notas, iCloud Drive, Mail (archivos adjuntos y el cuerpo completo del correo), Calendario (archivos adjuntos) y iCloud Keychain nativas. Este tipo de activación permite la administración de aplicaciones, la gestión de la política de TI, los perfiles de correo electrónico, los perfiles Wi-Fi y la VPN por aplicación. Los administradores pueden gestionar los datos del trabajo (por ejemplo, borrar datos del trabajo) sin perjudicar los datos personales. Este tipo de activación solo es compatible con los dispositivos iPhone y iPad sin supervisión.
Registro del dispositivo solo para BlackBerry 2FA	Este tipo de activación es compatible con la solución de BlackBerry 2FA para dispositivos que 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. No es compatible con los dispositivos Apple TV. Para obtener más información, consulte el contenido de BlackBerry 2FA.

Tipos de activación: dispositivos Android

Para los dispositivos 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 que admiten Samsung Knox Workspace reciben el primer tipo de activación y los que no admiten Samsung Knox Workspace reciben el segundo.

Dispositivos Android Management

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

Tipo de activación	Descripción
Trabajo y personal: privacidad de usuario (Android Management con perfil de trabajo)	Este tipo de activación conserva la privacidad de los datos personales, pero permite administrar los datos de trabajo con comandos y reglas de políticas de TI. Se crea un perfil de trabajo en el dispositivo que separa los datos de trabajo de los personales. Los datos personales y los datos de trabajo están protegidos mediante el cifrado y la autenticación de contraseña.

Tipo de activación	Descripción
Trabajo y personal: control total (dispositivo con Android Management completamente gestionado con perfil de trabajo)	Este tipo de activación le permite administrar todo el dispositivo con comandos y reglas de políticas de TI. Se crea un perfil de trabajo en el dispositivo que separa los datos de trabajo de los 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 UEM. Tras la activación, los dispositivos 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. Este tipo de activación requiere que el dispositivo se restablezca a la configuración predeterminada de fábrica antes de la activación. Si BlackBerry UEM Client se elimina o se borra el perfil de trabajo del dispositivo, este se restablece automáticamente a la configuración predeterminada de fábrica.
Solo espacio de trabajo (dispositivo con Android Management completamente gestionado)	Este tipo de activación 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 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 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. Este tipo de activación requiere que el dispositivo se restablezca a la configuración predeterminada de fábrica antes de la activación. Si UEM Client se elimina o se borra el perfil de trabajo del dispositivo, este se restablece automáticamente a la configuración predeterminada de fábrica.

Dispositivos 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 permite administrar los datos de trabajo con comandos y reglas de políticas de TI. Se crea un perfil de trabajo en el dispositivo que separa los datos de trabajo de los personales. Los datos personales y los datos de trabajo están protegidos mediante el cifrado y la autenticación de contraseña. Para permitir la gestión de aplicaciones Google Play para dispositivos Android Enterprise, seleccione "Añadir Google Play al espacio de trabajo" en el perfil de activación (habilitado de forma predeterminada). Si el dispositivo no tiene acceso a Google Play, el usuario debe descargar la última versión de UEM Client de una fuente diferente. Para descargar el archivo .apk de la versión más reciente de UEM Client, consulte KB 42607. 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 UEM Client.
Trabajo y personal: control total (dispositivo con 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. Se crea un perfil de trabajo en el dispositivo que separa los datos de trabajo de los 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 UEM. Para permitir la gestión de aplicaciones Google Play para dispositivos Android Enterprise, seleccione "Añadir cuenta de Google Play al espacio de trabajo" en el perfil de activación (habilitado de forma predeterminada). Tras la activación, los dispositivos 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. Para especificar si UEM puede limitar la activación por ID de dispositivo, seleccione "Permitir solo ID de dispositivo aprobados" 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 UEM Client se elimina o se borra el perfil de trabajo del dispositivo, este se restablece automáticamente a la configuración predeterminada de fábrica. Durante la activación los usuarios deberán conceder los permisos de administrador a UEM Client.

Tipo de activación	Descripción
Solo espacio de trabajo (dispositivo con Android Enterprise completamente gestionado)	Este tipo de activación permite administrar todo el dispositivo con comandos y reglas de políticas de TI. Se 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. Para permitir la gestión de aplicaciones Google Play para dispositivos Android Enterprise, seleccione "Añadir Google Play al espacio de trabajo" en el perfil de activación (habilitado de forma predeterminada). Si el dispositivo no tiene acceso a Google Play, el usuario puede descargar UEM Client mediante un archivo .apk de la aplicación. Puede configurar e incluir un QR Code que contenga la ubicación del archivo de origen de UEM Client en el mensaje de correo electrónico de activación que envíe a los usuarios. Cuando un usuario escanea el código QR Code, el UEM Client se descarga automáticamente. Para configurar e incluir un QR Code en el mensaje de correo electrónico de activación, debe seleccionar la casilla de verificación "Permitir códigos QR para la activación del dispositivo" en la página Valores predeterminados de activación (Configuración > Configuración general > Valores predeterminados de activación). También debe seleccionar la casilla de verificación "Permitir que el código QR contenga la ubicación del archivo de origen de la aplicación UEM Client" y especificar la ubicación del archivo de origen de la aplicación UEM Client. Para obtener el archivo .apk de la versión más reciente de UEM Client, consulte KB 42607. Durante la activación el dispositivo instala automáticamente 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 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. Para especificar si UEM puede limitar la activación por ID de dispositivo, seleccione "Permitir solo ID de dispositivo aprobados" 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 UEM Client se elimina o se borra el perfil de trabajo del dispositivo, este se restablece automáticamente a la configuración predeterminada de fábrica.

Dispositivos Android sin un perfil de trabajo

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

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. No se crea un contenedor independiente en el dispositivo. Para proporcionar seguridad a los datos del trabajo, puede instalar aplicaciones 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 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 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

Nota: 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, consulte KB 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 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. Se 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 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 Workspace y Knox MDM. Se 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. Durante la activación los usuarios deberán conceder los permisos de administrador a UEM Client.

Tipos de activación: dispositivos macOS

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

Tipos de activación: dispositivos Windows 10

Nota: Los dispositivos Windows 10 Mobile ya no son compatibles con Microsoft y solo tienen compatibilidad limitada en UEM.

Tipo de activación	Descripción
Controles de MDM	Este tipo de activación proporciona una gestión de dispositivos básica mediante controles de dispositivos proporcionados por dispositivos Windows 10. No se instala un espacio de trabajo separado en el dispositivo y no hay seguridad adicional para los datos de trabajo. Puede controlar el dispositivo a través de comandos y políticas de TI. Los usuarios de Windows 10 activan los dispositivos a través de las aplicaciones de acceso de trabajo de Windows 10.

Gestión de la configuración de activación

Puede gestionar la forma en que los usuarios activan los dispositivos, incluido si los usuarios necesitan una contraseña de activación o si pueden escanear un QR Code, el tiempo de validez de una contraseña de activación o QR Code y si los usuarios pueden activar varios dispositivos con la misma contraseña o QR Code.

Ajuste de la configuración de activación predeterminada

1. En la barra de menús de la consola de administración, haga clic en **Configuración > Configuración general > Valores predeterminados de activación**.
2. En la sección **Valores predeterminados de activación del dispositivo**, especifique la contraseña de activación y las opciones de QR Code.
3. Si desea que BlackBerry UEM notifique a un usuario con un mensaje de correo electrónico cada vez que se active un dispositivo en su cuenta, seleccione la casilla de verificación **Enviar notificación de dispositivo activado**.
4. Para permitir que los usuarios activen aplicaciones BlackBerry Dynamics con un QR Code, en la sección **Control predeterminado de la aplicación BlackBerry Dynamics**, seleccione la casilla de verificación **Usar códigos QR para desbloquear aplicaciones de BlackBerry Dynamics**. Para obtener más información, consulte Generación de claves de acceso, contraseñas de activación o códigos QR para aplicaciones de BlackBerry Dynamics.
5. Para simplificar la forma en que los usuarios activan sus dispositivos móviles, en la sección **BlackBerry Infrastructure**, seleccione la casilla de verificación **Activar registro con BlackBerry Infrastructure**. Si elimina la selección de esta opción, los usuarios deberán proporcionar la dirección del servidor para UEM al activar sus dispositivos.
6. Para importar o exportar una lista de ID de dispositivo aprobados, en la sección **Importar o exportar ID de los dispositivos**, haga clic en **Examinar**. Desplácese al archivo .csv que contiene una lista de ID de dispositivos aprobados y selecciónelo. Para obtener más información, consulte Importación o exportación de una lista de ID de los dispositivos aprobados.
7. Haga clic en **Guardar**.

Establezca una contraseña de activación y envíe un mensaje de correo de activación

Puede establecer una contraseña de activación y enviar un correo electrónico de activación a un usuario con instrucciones para activar uno o más dispositivos. En entornos locales, el correo se envía desde la dirección de correo electrónico que haya configurado en la configuración del servidor SMTP.

Antes de empezar: Creación de una plantilla de correo de activación.

1. En la barra de menús de la consola de administración, haga clic en **Usuarios > Dispositivos gestionados**.
2. Busque el nombre de una cuenta de usuario y haga clic en él.
3. En la sección **Detalles de activación**, haga clic en **Establecer contraseña de activación**.
4. En la lista desplegable **Opción de activación**, lleve a cabo una de las acciones siguientes:
   - Si desea que el usuario pueda activar su dispositivo con el perfil de activación que tiene actualmente asignado, seleccione **Activación del dispositivo predeterminada**.

- Si desea emparejar una contraseña de activación con un perfil de activación específico, seleccione **Activación del dispositivo con perfil de activación especificado**. Para obtener más información, consulte Permitir que los usuarios activen varios dispositivos con diferentes tipos de activación.

5. En la lista desplegable **Contraseña de activación**, lleve a cabo una de las acciones siguientes:
   - Si desea generar automáticamente una contraseña, seleccione **Generar automáticamente la contraseña de activación del dispositivo y enviar un correo electrónico con las instrucciones de activación**. Cuando se selecciona esta opción, deberá seleccionar una plantilla de correo para enviar la información al usuario.
   - Si desea establecer una contraseña de activación para el usuario y, opcionalmente, enviar un correo electrónico de activación, seleccione **Establecer contraseña de activación del dispositivo** y escriba una contraseña.
6. Opcionalmente, para especificar cuánto tiempo permanece válida la contraseña de activación, cambie la caducidad del periodo de activación.
7. Si desea que la contraseña de activación sea válida solo para una activación de dispositivo, seleccione **El periodo de activación caduca después de la activación del primer dispositivo**.
8. En la lista desplegable **Plantilla del correo de activación**, seleccione la plantilla de correo que desea usar.
9. Haga clic en **Submit**.

Envío de un mensaje de correo electrónico de activación a varios usuarios

Puede enviar mensajes de correo electrónico de activación a varios usuarios al mismo tiempo. Cuando envíe un mensaje de correo electrónico de activación a varios usuarios, la contraseña de activación se generará automáticamente. El correo se envía desde la dirección de correo que haya configurado en la configuración del servidor SMTP.

Antes de empezar: Creación de una plantilla de correo de activación.

1. En la barra de menús de la consola de administración, haga clic en **Usuarios > Dispositivos gestionados**.
2. Seleccione la casilla de verificación para cada usuario al que desee enviar un mensaje de correo electrónico de activación.
3. Haga clic en  .
4. En la lista desplegable **Opción de activación**, lleve a cabo una de las acciones siguientes:
   - Si desea que los usuarios puedan activar sus dispositivos con el perfil de activación que tienen actualmente asignado, seleccione **Activación del dispositivo predeterminada**.
   - Si desea emparejar una contraseña de activación con un perfil de activación específico, seleccione **Activación del dispositivo con perfil de activación especificado**. Para obtener más información acerca del emparejamiento de contraseñas de activación con perfiles de activación, consulte Permitir que los usuarios activen varios dispositivos con diferentes tipos de activación.
5. En la lista desplegable **Contraseña de activación**, seleccione **Generar automáticamente la contraseña de activación del dispositivo y enviar un correo electrónico con las instrucciones de activación**.
6. Para especificar durante cuánto tiempo es válida la contraseña de activación, cambie la caducidad del periodo de activación.
7. Si desea que la contraseña de activación sea válida solo para una activación de dispositivo, seleccione **El periodo de activación caduca después de la activación del primer dispositivo**.
8. En la lista desplegable **Plantilla del correo de activación**, seleccione la plantilla de correo que desea usar.
9. Haga clic en **Enviar**.

Permitir a los usuarios configurar contraseñas de activación en BlackBerry UEM Self-Service

Puede permitir a los usuarios con dispositivos iOS, Android y Windows crear sus propias contraseñas de activación mediante BlackBerry UEM Self-Service.

1. En la barra de menús de la consola de administración, haga clic en **Configuración > Autoservicio > Configuración de autoservicio**.
2. Seleccione la casilla de verificación **Permitir que los usuarios activen los dispositivos a través de la consola de autoservicio** y haga lo siguiente:
3. Especifique cuánto tiempo tiene un usuario para activar un dispositivo antes de que caduque la contraseña de activación.
4. Especifique el número mínimo de caracteres requeridos en una contraseña de activación.
5. En la lista desplegable **Complejidad mínima de la contraseña**, seleccione el nivel de complejidad requerido.
6. Para que se envíe automáticamente un correo electrónico de activación a los usuarios cuando crean una contraseña de activación, seleccione la casilla de verificación **Enviar un correo electrónico de activación**. En la lista desplegable **Plantilla del correo de activación**, seleccione una plantilla de correo electrónico.
7. Para enviar mensajes de activación personalizados a los usuarios, seleccione la casilla de verificación **Enviar mensajes de activación personalizados**. Seleccione una plantilla de mensaje para cada tipo de dispositivo de la lista desplegable adecuada.
8. Para enviar correos electrónicos de notificación de inicio de sesión a los usuarios cada vez que inician sesión en UEM Self-Service, seleccione la casilla de verificación **Enviar notificación de inicio de sesión de autoservicio**.
9. Haga clic en **Guardar**.

Permitir que los usuarios activen varios dispositivos con diferentes tipos de activación

Puede crear varias contraseñas de activación para un usuario y emparejar las contraseñas de activación con perfiles de activación específicos de modo que los usuarios puedan activar los dispositivos con diferentes tipos de activación.

Por ejemplo, es posible que desee que los usuarios activen dispositivos de trabajo con un tipo de activación que le permita tener control total de los dispositivos y que activen sus dispositivos personales con un tipo de activación que permita la privacidad del usuario. Mediante el emparejamiento de una contraseña de activación con un perfil de activación que permite el control total de los dispositivos y una segunda contraseña de activación con el perfil de activación de privacidad de usuario, los usuarios pueden activar cada dispositivo con diferentes resultados. Puede crear plantillas de correo que describan el uso previsto para cada contraseña.

Para emparejar una contraseña de activación con un perfil de activación específico, cuando cree una cuenta de usuario o envíe un mensaje de correo electrónico de activación, seleccione la opción "Activación del dispositivo con el perfil de activación especificado".

Puede tener un máximo de dos contraseñas de activación emparejadas con perfiles de activación específicos. Cada contraseña se puede usar para activar varios dispositivos. Tenga en cuenta que, para las contraseñas de activación que están emparejadas con perfiles de activación, la opción "Número de dispositivos que un usuario puede activar" del perfil de activación no se aplica.

Si elimina un perfil de activación emparejado con una contraseña de activación, dicha contraseña caduca automáticamente. Si es necesario, puede hacer que las contraseñas de activación caduquen para un usuario en cualquier momento.

Los usuarios no pueden crear contraseñas de activación que se emparejan con perfiles de activación específicos en BlackBerry UEM Self-Service.

Esta opción no es compatible con dispositivos iOS inscritos en DEP.

Forzado de la caducidad de la contraseña de activación

Puede hacer caducar manualmente una contraseña de activación que se generó para un usuario.

1. En la barra de menús de la consola de administración, haga clic en **Usuarios > Dispositivos gestionados**.
2. Busque el nombre de una cuenta de usuario y haga clic en él.
3. En la sección **Detalles de activación**, debajo de la contraseña de activación que desea que caduque, haga clic en **Caducar**.

La contraseña de activación caduca inmediatamente. Si fuerza la caducidad de una contraseña de activación normal, se muestra la fecha y la hora en que la contraseña ha caducado. Si fuerza la caducidad de una contraseña de activación que se emparejó con un perfil de activación específico, los detalles de la contraseña de activación del dispositivo ya no se muestran.

Compatibilidad de las activaciones de Android Enterprise y Android Management

La forma de activar los dispositivos Android Enterprise y Android Management de los usuarios puede depender de varios factores, como la versión de SO de Android del dispositivo y el grado de control que su organización desee tener sobre los dispositivos de los usuarios. También puede depender de si su empresa interactúa con servicios Google utilizando cuentas Google Playgestionadas, dominios de Google Workspace o dominios de Google Cloud, o si no utiliza servicios Google.

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

Si su empresa no tiene un dominio de Google o usted no quiere conectar BlackBerry UEM a su dominio de Google, puede activar dispositivos Android Enterprise y Android Management con cuentas gestionadas de Google Play. Las cuentas gestionadas de Google Play permiten añadir aplicaciones internas a Google Play que pueden descargar los usuarios de dispositivos Android Enterprise.

Para usar cuentas gestionadas de Google Play con UEM, utilice cualquier cuenta de Google o Gmail para conectar UEM con Google. No se envía ninguna información personal identificable sobre los usuarios a Google. Cuando haya conectado UEM a Google, podrá permitir que los usuarios activen los dispositivos Android Enterprise y Android Management y descarguen aplicaciones de trabajo mediante Google Play. Para obtener información acerca de la configuración de UEM para que sea compatible con los dispositivos Android Enterprise Android Management, consulte Configuración de BlackBerry UEM para que admita dispositivos Android Enterprise y Configuración de BlackBerry UEM para que admita dispositivos Android Management.

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

Si ha configurado BlackBerry UEM para conectarse al dominio de Google Workspace de su empresa, debe realizar las siguientes tareas antes de que los usuarios puedan activar los dispositivos Android Enterprise.

Antes de empezar: Configuración de BlackBerry UEM para que admita dispositivos Android Enterprise.

1. En el dominio de Google Workspace, cree cuentas de usuario para los usuarios de Android.
2. Seleccione la configuración **Aplicar política de EMM**.

   Esta configuración es necesaria para los dispositivos a los que se asignarán los tipos de activación Solo espacio de trabajo y Trabajo y personal: control total, y se recomienda encarecidamente para los 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. En 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 Google Workspace correspondiente.
4. En 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: Configuración de BlackBerry UEM para que admita dispositivos Android Enterprise. Cuando se configura UEM para conectarse a un dominio de Google Cloud, debe seleccionar si 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.

1. En UEM, añada las cuentas de usuario del directorio para los usuarios de Android Enterprise.
2. Si elige no permitir a UEM crear cuentas de usuario en el dominio de Google Cloud, deberá crear cuentas de usuario en el dominio de Google Cloud y en UEM. Lleve a cabo una de estas 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 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 los dispositivos con los tipos de activación Solo espacio de trabajo y Trabajo y personal: control total y se recomienda encarecidamente para los 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 UEM, asigne un perfil de correo electrónico y aplicaciones de productividad a los usuarios, grupos de usuarios o grupos de dispositivos.

Compatibilidad de los 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 activarán con los tipos de activación Solo espacio de trabajo o Trabajo y personal: control total, el dispositivo debe establecerse a los valores predeterminados de fábrica antes de instalar UEM Client. Puede incluir una ubicación de descarga especificada en un QR Code.
- 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. Para estos dispositivos, una vez finalizada la configuración inmediata, los usuarios pueden instalar UEM Client.

Para descargar el archivo .apk de la versión más reciente de UEM Client, consulte KB 42607.

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

Requisito	Descripción
Entorno de BlackBerry UEM	Si solo desea admitir dispositivos que no tienen acceso a Google Play, no es necesario que integre su entorno de UEM en Android Enterprise. Si quiere admitir dispositivos que tengan y no tengan acceso a Google Play, debe integrar el entorno en Android Enterprise.
Configuración de activación predeterminada	Si desea incluir la ubicación de UEM Client en un código QR, en la configuración de activación predeterminada, seleccione "Permitir que el código QR contenga la ubicación del archivo de origen de la aplicación de 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 descargas de BlackBerry. Esas opciones solo están disponibles si su entorno UEM está integrado con Android Enterprise.
Configuración del perfil de activación	Compruebe los siguientes ajustes del perfil de activación: • Desmarque la opción "Añadir cuenta de Google Play al espacio de trabajo". • 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 una aplicación interna y asignarla a usuarios.
Reglas de políticas de TI	Para los usuarios que tengan asignado el tipo de activación Trabajo y personal: privacidad de usuario (Android Enterprise), para permitir la instalación de aplicaciones fuera de Google Play, active la regla de política de TI "Permitir instalación de aplicaciones que no sean 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 aplicaciones internas y asígnelas a usuarios. 1. Obtenga los archivos .apk de las aplicaciones que desee asignar. 2. En la barra de menús de la consola de administración, haga clic en **Aplicaciones**. 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. Para instalar o actualizar aplicaciones internas en dispositivos que no tengan acceso a Google Play, debe hacer lo siguiente: **1.** Obtenga los archivos .apk de las aplicaciones de BlackBerry Dynamics que desee asignar. **2.** En la barra de menús de la consola de administración, haga clic en **Aplicaciones**. **3.** Haga clic en una aplicación de BlackBerry Dynamics. **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 de BlackBerry UEM Client	Para actualizar la aplicación de UEM Client en los dispositivos, los usuarios deben descargar manualmente la versión más reciente del archivo .apk e instalarla.

Ayuda con las activaciones de Windows 10

Puede ayudar a los usuarios a activar los dispositivos Windows 10 de las siguientes formas:

- Cree o edite una plantilla de correo de activación para proporcionar la información de activación de Windows 10. Para obtener más información, consulte Creación de una plantilla de correo de activación.
- Integración de UEM con Entra ID : cuando se configura la combinación de Entra ID, los usuarios pueden activar sus dispositivos utilizando únicamente su nombre de usuario y contraseña de Entra ID.
- Configuración de Windows Autopilot: cuando se configura Windows Autopilot, la inscripción forma parte de la experiencia de configuración inicial y el dispositivo se activa automáticamente cuando el usuario la completa utilizando únicamente su nombre de usuario y contraseña de Entra ID.
- Implementación de un servicio de detección: puede utilizar una aplicación web de Java de BlackBerry como un servicio de detección para simplificar el proceso de activación para los usuarios con dispositivos Windows 10. Si utiliza el servicio de detección, los usuarios no necesitan escribir una dirección de servidor durante el proceso de activación.

Compatibilidad de la inscripción de usuario de Apple para dispositivos con iOS y iPadOS

Puede utilizar el tipo de activación Privacidad de usuario: inscripción de usuario para los dispositivos iOS y iPadOS con el fin de garantizar que los datos del usuario se mantengan privados y separados de los datos del trabajo. Con este tipo de activación, se instala un espacio de trabajo independiente en el dispositivo para las aplicaciones de trabajo y las aplicaciones Notas, iCloud Drive, Mail (archivos adjuntos y el cuerpo completo del correo), Calendario (archivos adjuntos) y iCloud Keychain nativas. Este tipo de activación permite la administración de aplicaciones, la gestión de la política de TI, los perfiles de correo electrónico, los perfiles Wi-Fi y la VPN por aplicación. Los administradores pueden gestionar los datos del trabajo (por ejemplo, borrar datos del trabajo) sin perjudicar los datos personales. Este tipo de activación es compatible con los dispositivos iPhone y iPad no supervisados que ejecuten versiones compatibles de iOS o iPadOS.

Si desea admitir la inscripción de usuario de Apple, haga lo siguiente:

- Compruebe que los dispositivos que activará utilizando este tipo de activación no están supervisados.
- Cree una cuenta de Apple ID gestionada para cada usuario. La dirección de correo electrónico de la cuenta de Apple ID gestionada debe coincidir con la dirección de correo electrónico del usuario en BlackBerry UEM.
- Cuando establezca la contraseña de activación del dispositivo para un usuario, seleccione la plantilla de correo de activación de inscripción de usuario de Apple.
- Si desea que los usuarios puedan activar fácilmente otras aplicaciones BlackBerry Dynamics, importar certificados, utilizar funciones de BlackBerry 2FA, utilizar CylancePROTECT y comprobar su estado de conformidad con facilidad, asigne BlackBerry UEM Client utilizando una licencia VPP. Si indica Obligatorio para esta disposición, se le solicita al usuario que instale la aplicación. Si indica Opcional para esta disposición, el usuario debe descargar manualmente la aplicación de las aplicaciones de trabajo.

Compatibilidad con Samsung Knox DualDAR

Los dispositivos compatibles con el cifrado Samsung Knox DualDAR pueden proteger los datos de trabajo utilizando dos capas de cifrado. La capa exterior de Knox DualDAR está desarrollada a partir del cifrado basado en archivos de Android y mejorada por Samsung para cumplir con los requisitos de la MDFPP. En el perfil de activación, puede especificar si utiliza la aplicación de cifrado integrada predeterminada o una aplicación de cifrado interna que desea utilizar para la capa interior del cifrado del perfil de trabajo.

Si decide utilizar la aplicación predeterminada, el perfil de trabajo se protege mediante un módulo criptográfico certificado FIPS 140-2 incluido en el marco de Samsung Knox. La aplicación de cifrado interna es un módulo criptográfico creado expresamente y desarrollado por su empresa o por terceros y del que se espera que tenga certificación FIPS 140-2. Cuando el usuario no está utilizando el dispositivo, todos los datos del perfil de trabajo se bloquean y se vuelven inaccesibles para las aplicaciones que se estén ejecutando en segundo plano.

Requisito	Descripción
Dispositivos compatibles	Compatibilidad con modelos insignia de Samsung.
Aplicación de cifrado	Si tiene una aplicación de cifrado que quiera utilizar para el cifrado Knox DualDAR, debe añadirla como una aplicación interna en la consola de administración. Seleccione esta aplicación de cifrado cuando cree un perfil de activación para los dispositivos que sean compatibles con Knox DualDAR. De forma alternativa, puede seleccionar la aplicación de cifrado predeterminada.
Perfil de activación	Si habilita el cifrado de Knox DualDAR en el perfil de activación, debe asignar el perfil únicamente a los dispositivos que sean compatibles. Si su empresa es compatible con distintos dispositivos que podrían ser o no compatibles con Knox DualDAR, debe asignar el perfil de activación a un grupo de dispositivos. Si habilita la activación de Knox DualDAR para un dispositivo no compatible, la activación no se completará con éxito. Para permitir la compatibilidad con el cifrado Knox DualDAR, cree un perfil de activación con la siguiente configuración para los dispositivos Android: • Seleccione el tipo de activación Trabajo y personal: control total (dispositivo completamente gestionado con Android Enterprise con perfil de trabajo). • Seleccione la opción "Al activar dispositivos Android Enterprise, active las funciones premium de UEM como BlackBerry Secure Connect Plus". • Seleccione la opción "Activar Samsung Knox DualDAR Workspace". • Para utilizar la aplicación de cifrado predeterminada, seleccione la opción "Aplicación de cifrado integrada predeterminada". Para utilizar otra aplicación de cifrado, seleccione la opción "Seleccionar una aplicación interna para el cifrado" y elija la aplicación de cifrado que desee en la lista de aplicaciones.
BlackBerry UEM Client	Se recomienda la versión más reciente de BlackBerry UEM Client para Android.

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 el número de dispositivos y los tipos de dispositivos que un usuario puede activar, así como el tipo de activación que se debe utilizar para cada tipo de dispositivo. El tipo de activación determina el grado de control que se tiene sobre los dispositivos activados.

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 adaptarlo a 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 de la consola de administración, haga clic en **Políticas y perfiles > Política > Activación**.
2. Haga clic en +.
3. Escriba un nombre y una descripción para el perfil.
4. En el campo **Número de dispositivos que un usuario puede activar**, especifique el número máximo de dispositivos que puede activar un usuario.
5. En la lista desplegable **Propietario del dispositivo**, seleccione una de las siguientes opciones:
   - Si algunos usuarios activan dispositivos personales y algunos usuarios activan los dispositivos de trabajo, seleccione **No especificado**.
   - Si la mayoría de los usuarios activan dispositivos de trabajo, seleccione **Trabajo**.
   - Si la mayoría de los usuarios activan dispositivos personales, seleccione **Personal**.
6. Opcionalmente, en la lista desplegable **Asignar aviso de la empresa**, seleccione un aviso de empresa. 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.
7. En la sección **Tipos de dispositivo que los usuarios pueden activar**, seleccione los tipos de SO del dispositivo según sea necesario.
8. Para cada tipo de dispositivo que incluya en el perfil de activación, realice las siguientes acciones:
   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.
      - **No permitir modelos de dispositivo seleccionados**: los usuarios no pueden activar los modelos de dispositivo especificados.

      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.
   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.

Nota: Debe crear perfiles de activación independientes para Android Enterprise y Android Management. Si se especifican tipos de activación Android Enterprise y Android Management en el mismo perfil, el tipo Android Management tendrá prioridad aunque esté clasificado por debajo de Android Enterprise. Solo la contraseña y la información de activación del tipo de activación Android Management se incrustarán en el código QR.

9. Para dispositivos con iOS y iPadOS, lleve a cabo las siguientes acciones:
   a) Si ha seleccionado el tipo de activación Privacidad del usuario y desea activar las licencias basadas en SIM, debe seleccionar **Permitir el acceso a la tarjeta SIM y a la información del hardware del dispositivo para activar licencias basadas en SIM**.
   b) Si ha seleccionado el tipo de activación Privacidad del usuario y desea administrar funciones específicas, seleccione las casillas de verificación correspondientes.
   c) Si ha seleccionado Controles de MDM o los tipos de activación Privacidad del usuario (con licencias basadas en SIM) y solo desea activar dispositivos supervisados, seleccione **No permitir activar dispositivos no supervisados**.
   d) Opcionalmente, en la sección **Comprobar la integridad de la aplicación de iOS**, seleccione uno de los siguientes métodos de atestación:

      - **Realizar la comprobación de la integridad de la aplicación en la activación de la aplicación de BlackBerry Dynamics**: use este método para enviar comprobaciones a los dispositivos cuando se activen para verificar la integridad de las aplicaciones de trabajo de iOS.
      - **Realizar comprobaciones de la integridad de la aplicación periódicas**: use este método para enviar comprobaciones a los dispositivos para verificar la integridad de las aplicaciones de trabajo de iOS.

      Para realizar la comprobación de integridad de la aplicación de iOS, debe activar CylancePROTECT en su dominio de UEM. Para obtener más información, consulte Habilitar CylancePROTECT Mobile en su dominio de UEM.
   e) Opcionalmente, en la sección **Atestación de dispositivos gestionados**, seleccione uno de los siguientes métodos de atestación:

   - **Realizar la atestación de dispositivos gestionados al activar los dispositivos**: use este método para enviar comprobaciones a los dispositivos cuando se activen para verificar la integridad de las propiedades de los dispositivos.
   - **Realizar la atestación periódica de dispositivos gestionados**: use este método para enviar comprobaciones periódicamente para verificar la integridad de las propiedades de los dispositivos.

   Para realizar la atestación de dispositivos gestionados en dispositivos iOS, debe activar la función. Para obtener más información, consulte Configuración de la atestación para dispositivos iOS en el contenido de Administración.

   La atestación de dispositivos gestionados se aplica a los tipos de activación Controles de MDM y Privacidad del usuario, pero no al tipo de activación Privacidad de usuario: inscripción de usuario. Cuando selecciona el tipo de activación Privacidad del usuario, debe seleccionar al menos una de las opciones de administración (como "Permitir administración de VPN").
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.
   b) 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.

c) Si ha seleccionado un tipo de activación Android Enterprise, seleccione las opciones de Android Enterprise correspondientes:

- Para activar las funciones BlackBerry Secure Connect Plus y Knox de Platform for Enterprise (para los dispositivos compatibles con Samsung Knox) en dispositivos con una licencia adecuada, seleccione **Al activar dispositivos Android Enterprise, active las funciones premium de UEM como BlackBerry Secure Connect Plus**.
- Para activar el cifrado Samsung Knox DualDAR en los dispositivos que lo admiten, seleccione **Activar Samsung KNOX DualDAR Workspace**.
- Para permitir la administración de la aplicación Google Play en el espacio de trabajo, seleccione **Agregar cuenta de Google Play al espacio de trabajo**.
- Para permitir que UEM restrinja la activación por ID de dispositivo, seleccione **Permitir solo ID de dispositivo aprobados**. Esta opción solo es compatible con los dispositivos con Solo espacio de trabajo y Trabajo y personal: control total.
- Para especificar el tipo de red a través del cual los usuarios pueden activar un dispositivo, en la lista desplegable **Inscripción mediante código QR**, seleccione una red. Esta opción solo es compatible con los dispositivos con Solo espacio de trabajo y Trabajo y personal: control total.

d) Opcionalmente, en la sección **Opciones de atestación de SafetyNet o Play Integrity**, seleccione uno de los siguientes métodos de atestación:

- **Realizar la atestación de SafetyNet o Play Integrity 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 (solo se aplica a las versiones de UEM Client que no son compatibles con Play Integrity)**: utilice este método para enviar comprobaciones y poner a prueba la autenticidad y la integridad de los dispositivos cuando se activan.
- **Realizar la atestación de SafetyNet o Play Integrity 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.

e) Si desea que UEM envíe comprobaciones a los dispositivos cuando se activen para garantizar que se ha instalado el nivel de parche de seguridad requerido, en la sección **Opciones de atestación de hardware**, seleccione **Aplicar reglas de cumplimiento de atestación durante la activación**.

11. Para dispositivos con Windows 10, seleccione una o ambas opciones de factor de forma.

12. Haga clic en **Agregar**.

Después de terminar:

- Si fuera necesario, clasifique los perfiles de activación.
- Asigne el perfil a las cuentas y grupos de usuarios.

Activación de dispositivos Android

Los pasos que siguen los usuarios para instalar el BlackBerry UEM Client y activar los dispositivos Android dependen de varios factores, como la versión del sistema operativo de Android, el fabricante del dispositivo, la forma en que su empresa utiliza los servicios de Google, el tipo de activación especificado en el perfil de activación del dispositivo y las preferencias de su empresa. Puede proporcionar instrucciones de activación del dispositivo en el correo electrónico de activación que envíe a los usuarios. Para obtener más información sobre la creación de una plantilla de correo electrónico de activación, consulte Creación de una plantilla de correo electrónico de activación.

Los dispositivos Android Management admiten los siguientes métodos de activación:

Método de activación	Descripción
Activación para la privacidad del usuario de Android Management	En el caso de los dispositivos que se activarán con el tipo de activación Trabajo y personal: privacidad de usuario, los usuarios pueden configurar un perfil de trabajo y utilizar un código QR proporcionado para descargar UEM Client desde Google Play y activar el dispositivo en UEM. Para obtener más información, consulte Activación de un dispositivo Android Management con el tipo de activación de Trabajo y personal: privacidad de usuario.
Activación para control total de Android Management y solo espacio de trabajo	En el caso de los dispositivos que se activarán con los tipos de activación Trabajo y personal: control total y Solo espacio de trabajo, el usuario debe restablecer el dispositivo a los valores predeterminados de fábrica y utilizar un código QR proporcionado para descargar el UEM Client desde Google Play y activar el dispositivo en UEM. Para obtener más información, consulte Activación de un dispositivo Android Management mediante una cuenta de Google Play gestionada.

Los dispositivos Android Enterprise admiten los siguientes métodos de activación:

Método de activación	Descripción
Instale el 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 desde Google Play. Para obtener más información, consulte Activación de un dispositivo Android Enterprise con el tipo de activación Trabajo y personal: privacidad de usuario.
Descargue el archivo .apk de UEM Client desde el sitio de descarga de BlackBerry.	Si los usuarios de Android no tienen acceso a Google Play, para los dispositivos que se activarán con el tipo de activación Trabajo y personal: privacidad de usuario, los usuarios pueden descargar el archivo .apk de UEM Client desde el sitio de descarga de BlackBerry. También puede descargar el archivo desde BlackBerry y colocarlo en una ubicación a la que sus usuarios puedan acceder. Para obtener el archivo .apk de la versión más reciente de UEM Client, consulte KB 42607.

Método de activación	Descripción
Utilice las credenciales del dominio de Google durante la configuración del dispositivo.	Si BlackBerry UEM está conectado al dominio de Google Workspace 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.
Escanee un código QR que contenga la ubicación de descarga de UEM Client.	BlackBerry UEM le permite incluir la ubicación de descarga de UEM Client en un código QR que puede incluir en el correo electrónico de activación que envíe a los usuarios. Los usuarios que están asignados a Solo espacio de trabajo o Trabajo y personal: control total pueden escanear el código QR para descargar UEM Client. Para obtener más información, consulte Activación de un dispositivo Android Enterprise mediante una cuenta de Google Play gestionada.
Aprovisionamiento automático de Android o Samsung Knox Mobile Enrollment.	El aprovisionamiento automático de Android le permite implementar un gran número de dispositivos Android Enterprise a la vez. Knox Mobile Enrollment le permite activar un gran número de dispositivos Samsung Knox con activaciones Android Enterprise. Para utilizar esta opción, los dispositivos deben estar preparados para el aprovisionamiento automático o Knox Mobile Enrollment al adquirirlos de un distribuidor autorizado. Para obtener más información, consulte Configuración de la compatibilidad con el aprovisionamiento automático de Android o Active varios dispositivos mediante Knox Mobile Enrollment.

En el caso de los dispositivos Android Enterprise, cada opción de activación 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	Privacidad del usuario de AE	Control total de AE			Solo espacio de trabajo de AE		
Método		Dominio de Google	Google Play administrado	Sin acceso a Google	Dominio de Google	Google Play administrado	Sin acceso a Google
Instalar UEM Client desde Google Play o descargar por el usuario	Sí	No	No	No	No	No	No
Credenciales de dominio de Google	Sí	Sí	No	No	Sí	No	No

Tipo de activación	Privacidad del usuario de AE	Control total de AE			Solo espacio de trabajo de AE		
Método		Dominio de Google	Google Play administrado	Sin acceso a Google	Dominio de Google	Google Play administrado	Sin acceso a Google
Escanear código QR	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Aprovisionamie automático de Android/Samsu Knox Mobile Enrollment	No	Sí	Sí	Sí	Sí	Sí	Sí

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

Para activar dispositivos con el tipo de activación Trabajo y personal: privacidad de usuario (Android Enterprise), envíe las siguientes instrucciones al usuario del dispositivo. Los dispositivos con este tipo de activación no requieren que se restablezcan los valores predeterminados de fábrica para su activación.

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 código QR de activación, puede utilizarlo para activar el dispositivo. Si no ha recibido un código QR, asegúrese de que tiene la siguiente información:

- Dirección de correo electrónico del trabajo
- Su nombre de usuario de UEM (normalmente, el nombre de usuario del trabajo)
- Su contraseña de activación de UEM
- La dirección del servidor de 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 mediante un archivo .apk. Para obtener el archivo .apk de la versión más reciente de UEM Client, consulte KB 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
Escanee un código QR para activar el dispositivo.	**a.** Toque . **b.** Toque **Permitir** para permitir que UEM Client haga fotos y grabe vídeos. **c.** Escanee el código QR que le proporcionó su administrador en el correo electrónico de activación.

Tarea	Pasos
Active manualmente el dispositivo.	**a.** Escriba su dirección de correo de trabajo y toque **Siguiente**. **b.** Escriba la contraseña de activación y toque **Activar mi dispositivo**. **c.** Si es necesario, escriba la dirección del servidor y toque **Siguiente**. **d.** Si es necesario, escriba su nombre de usuario y la contraseña de activación y toque **Siguiente**.

5. Toque **Permitir** para que UEM Client realice y administre llamadas telefónicas.
6. En la pantalla **Configura tu perfil**, toque **Configurar**. La configuración del perfil de trabajo puede tardar unos instantes.
7. Si se le solicita, inicie sesión en su cuenta de Google con su dirección de correo electrónico y su contraseña de Google.
8. Elija un método de desbloqueo de pantalla.
9. Si en la pantalla **Inicio seguro** se le solicita que requiera una contraseña cuando se inicie el dispositivo, toque **Sí**.
10. Escriba una contraseña del dispositivo y vuelva a escribirla para confirmarla. Toque **Aceptar**.
11. Seleccione cómo desea que se muestren las notificaciones. Toque **Hecho**.
12. 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.
13. Toque **Inscribirse**.
14. Si desea configurar la autenticación de huella dactilar para las aplicaciones UEM Client y BlackBerry Dynamics, siga las instrucciones que aparecen en pantalla. De lo contrario, toque **Cancelar**.
15. Si se ha cerrado la sesión en su dispositivo, desbloquéelo para completar la activación de UEM.
16. Si se le solicita, toque **Aceptar** para permitir la conexión con BlackBerry Secure Connect Plus y espere a que se active la conexión.
17. Si se le pide que instale aplicaciones de trabajo en su dispositivo, siga las instrucciones que aparecen en pantalla.

Después de terminar: Para verificar que el proceso de activación se haya 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 tengan asignado el tipo de activación Solo espacio de trabajo (Android Enterprise) o Trabajo y personal: control total (Android Enterprise) cuando BlackBerry UEM se conecte a un dominio de Google Workspace 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 Trabajo y personal: privacidad de usuario.

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, por lo que no tendrá que introducir ninguna información. Si no ha recibido un QR Code, asegúrese de que ha recibido la siguiente información:

- Dirección de correo electrónico del trabajo
- Su nombre de usuario de UEM (normalmente, el nombre de usuario del trabajo)
- Su contraseña de activación de UEM
- La dirección del servidor de 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 vídeo. **c.** Escanee el QR Code en el mensaje del correo electrónico 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 **Configura tu perfil**, toque **Configurar**. La configuración del perfil de trabajo puede tardar unos instantes.
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 y para cualquier aplicación de BlackBerry Dynamics que tenga. De lo contrario, toque **Cancelar**.
15. Si se ha cerrado la sesión en su dispositivo, desbloquéelo para completar la activación de 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 haya 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 mediante una cuenta de Google Play gestionada

Las siguientes instrucciones de activación se aplican a los dispositivos Android compatibles a los que se haya asignado el tipo de activación Solo espacio de trabajo (Android Enterprise) o Trabajo y personal: control total (Android Enterprise). Para activar dispositivos que estén conectados a una cuenta de Google Play gestionada con el tipo de activación Android Enterprise Trabajo y personal: privacidad de usuario, consulte Activación de un dispositivo Android Enterprise con el tipo de activación Trabajo y personal: privacidad de usuario.

Puede configurar e incluir un QR Code que contenga la ubicación del archivo de origen de la aplicación UEM Client en el mensaje de correo electrónico de activación que envíe a los usuarios. Cuando un usuario escanea el código QR Code, el UEM Client se descarga automáticamente. Para configurar e incluir un QR Code en el mensaje de correo electrónico de activación, debe seleccionar la casilla de verificación "Permitir códigos QR para la activación del dispositivo" en la página Valores predeterminados de activación (**Configuración > Configuración general > Valores predeterminados de activación**). También debe seleccionar la casilla de verificación "Permitir que el código QR contenga la ubicación del archivo de origen de la aplicación UEM Client" y especificar la ubicación del archivo de origen de la aplicación UEM Client. Para obtener el archivo .apk de la versión más reciente de UEM Client, consulte KB 42607.

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 que desea activar, si no ve la pantalla de configuración del dispositivo, restablezca los valores predeterminados de fábrica.
2. Para abrir el lector QR Code del dispositivo, toque la pantalla del dispositivo siete veces.
3. Para descargar el UEM Client, escanee el QR Code proporcionado por el administrador en el correo electrónico de activación.
4. Abra UEM Client.
5. Lea el acuerdo de licencia y toque la casilla de verificación **Acepto el acuerdo de licencia**.
6. En la pantalla **Configura tu perfil**, toque **Configurar**. La configuración del perfil de trabajo puede tardar unos instantes.
7. Elija un método de desbloqueo de pantalla.

8. Si en la pantalla **Inicio seguro** se le solicita que requiera una contraseña cuando se inicie el dispositivo, toque **Sí**.
9. Escriba la contraseña del dispositivo, repítala para confirmarla y, después, toque **Aceptar**.
10. Seleccione 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. Toque **Inscribirse**.
13. Si desea configurar la autenticación de huella dactilar para las aplicaciones UEM Client y BlackBerry Dynamics, siga las instrucciones que aparecen en pantalla. De lo contrario, toque **Cancelar**.
14. Si se ha cerrado la sesión en su dispositivo, desbloquéelo para completar la activación de UEM.
15. Si se le solicita que permita la conexión a BlackBerry Secure Connect Plus, toque **Aceptar** y espere a que se active la conexión.
16. Si se le pide que instale aplicaciones de trabajo en su dispositivo, siga las instrucciones que aparecen en pantalla.

Después de terminar: Para verificar que el proceso de activación se haya 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

Las siguientes instrucciones de activación se aplican a los dispositivos que tienen asignados los tipos de activación Solo espacio de trabajo (Android Enterprise) y Trabajo y personal: control total (Android Enterprise) y que no tienen acceso a Google Play. El usuario puede descargar BlackBerry UEM Client utilizando un archivo .apk de la aplicación. Puede configurar e incluir un QR Code que contenga la ubicación del archivo de origen de UEM Client en el mensaje de correo electrónico de activación que envíe a los usuarios. Cuando un usuario escanea el código QR Code, el UEM Client se descarga automáticamente.

Para configurar e incluir un QR Code en el mensaje de correo electrónico de activación, debe seleccionar la casilla de verificación "Permitir códigos QR para la activación del dispositivo" en la página Valores predeterminados de activación (**Configuración > Configuración general > Valores predeterminados de activación**). También debe seleccionar la casilla de verificación "Permitir que el código QR contenga la ubicación del archivo de origen de la aplicación UEM Client" y especificar la ubicación del archivo de origen de la aplicación UEM Client. Para obtener el archivo .apk de la versión más reciente de UEM Client, consulte KB 42607.

Envíe las instrucciones de activación siguientes a los usuarios 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 su administrador le ha enviado un QR Code de activación, puede usarlo para activar el dispositivo. Si no ha recibido un QR Code, asegúrese de que ha recibido la siguiente información:

- Dirección de correo electrónico del trabajo
- Su nombre de usuario de UEM (normalmente, el nombre de usuario del trabajo)
- Su contraseña de activación de UEM
- La dirección del servidor de UEM (si es necesario)

1. En el dispositivo que desea activar, si no ve la pantalla de configuración del dispositivo, restablezca los valores predeterminados de fábrica.
2. Para abrir el lector QR Code del dispositivo, toque la pantalla del dispositivo siete veces.
3. Para descargar el UEM Client, analice el QR Code que le proporcionó el administrador en el mensaje de correo electrónico de activación.
   El UEM Client se descarga automáticamente en el dispositivo.
4. Abra UEM Client.
5. Lea el acuerdo de licencia y toque la casilla de verificación **Acepto el acuerdo de licencia**.
6. Lleve a cabo una de estas acciones:

Tarea	Pasos
Utilice un QR Code para activar el dispositivo.	**a.** En UEM Client, toque . **b.** Toque **Permitir** para permitir que UEM Client haga fotos y grabe vídeos.
Active manualmente el dispositivo.	**a.** Escriba su dirección de correo de trabajo y toque **Siguiente**. **b.** Escriba la contraseña de activación y toque **Activar mi dispositivo**. **c.** Si es necesario, escriba la dirección del servidor y toque **Siguiente**. **d.** Si es necesario, escriba su nombre de usuario y la contraseña de activación y toque **Siguiente**.

7. En la pantalla **Configura tu perfil**, toque **Configurar**. La configuración del perfil de trabajo puede tardar unos instantes.
8. Elija un método de desbloqueo de pantalla.
9. Si en la pantalla **Inicio seguro** se le solicita que requiera una contraseña cuando se inicie el dispositivo, toque **Sí**.
10. Escriba una contraseña del dispositivo y vuelva a escribirla para confirmarla. Toque **Aceptar**.
11. Seleccione cómo desea que se muestren las notificaciones. Toque **Hecho**.
12. 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.
13. En la siguiente pantalla, toque **Inscribir**.
14. Si desea configurar la autenticación de huella dactilar para las aplicaciones UEM Client y BlackBerry Dynamics, siga las instrucciones que aparecen en pantalla. De lo contrario, toque **Cancelar**.
15. Si se ha cerrado la sesión en su dispositivo, desbloquéelo para completar la activación de UEM.
16. Si se le pide que permita la conexión a BlackBerry Secure Connect Plus, toque **Aceptar** y espere a que se active la conexión.
17. Si se le pide que instale aplicaciones de trabajo en su dispositivo, siga las instrucciones que aparecen en pantalla.
18. Si fuera necesario, para configurar el correo electrónico en su teléfono, abra la aplicación de correo electrónico que su empresa desea que utilice y siga las instrucciones.

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

Puede incluir un QR Code en el mensaje de correo electrónico de activación que envíe a los usuarios. Cuando un usuario escanea el código QR Code, el UEM Client se descarga automáticamente. Para configurar e incluir un

QR Code en el mensaje de correo electrónico de activación, debe seleccionar la casilla de verificación "Permitir códigos QR para la activación del dispositivo" en la página Valores predeterminados de activación (Configuración > Configuración general > Valores predeterminados de activación). Utilice la plantilla de correo electrónico de activación predeterminada de Android Management (o un equivalente personalizado).

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, vaya a **Configuración > Servicios y preferencias de Google**.
2. Toque **Configurar y restaurar**.
3. Toque **Configurar su perfil de trabajo**.
4. Toque **Siguiente**.
5. En el cuadro de diálogo **Permitir que la política del dispositivo tome fotografías y grabe vídeos**, toque **Solo esta vez**.
6. Escanee el código QR que ha recibido de su administrador.
7. Toque **Acepto**.
8. Toque **Siguiente**.
9. En función de cómo haya configurado el administrador la activación, es posible que se le solicite que establezca un bloqueo para el dispositivo o para el espacio de trabajo.
10. En la pantalla **Su lista de comprobación de trabajo**, situada debajo de **Instalar aplicaciones de trabajo**, toque **Instalar**.
11. Una vez instalado UEM Client, toque **Listo**.
12. Toque **Configurar BlackBerry UEM**.
13. Lea el contrato de licencia y toque **Acepto**.

El dispositivo terminará de configurar el perfil de trabajo.

Después de terminar: Si alguna vez desea desactivar el dispositivo y eliminarlo de UEM, puede hacerlo desde UEM Client.

Activación de un dispositivo Android Management mediante una cuenta de Google Play gestionada

Las siguientes instrucciones de activación se aplican a los dispositivos Android asignados al tipo de activación Trabajo y personal: control total (Android Management) o Solo espacio de trabajo (Android Management). Para activar dispositivos que estén conectados a una cuenta de Google Play gestionada con el tipo de activación Android Management Trabajo y personal: privacidad de usuario, consulte Activación de un dispositivo Android Management con el tipo de activación de Trabajo y personal: privacidad de usuario.

Puede incluir un QR Code en el mensaje de correo electrónico de activación que envíe a los usuarios. Cuando un usuario escanea el código QR Code, el UEM Client se descarga automáticamente. Para configurar e incluir un QR Code en el mensaje de correo electrónico de activación, debe seleccionar la casilla de verificación "Permitir códigos QR para la activación del dispositivo" en la página Valores predeterminados de activación (**Configuración > Configuración general > Valores predeterminados de activación**). Utilice la plantilla de correo electrónico de activación predeterminada de Android Management (o un equivalente personalizado).

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 que desea activar, si no ve la pantalla de configuración del dispositivo, restablezca los valores predeterminados de fábrica.
2. Para abrir el lector QR Code del dispositivo, toque la pantalla del dispositivo siete veces.
3. Para descargar el UEM Client, analice el QR Code que le proporcionó el administrador en el mensaje de correo electrónico de activación.
   El UEM Client se descarga automáticamente.
4. Abra UEM Client.
5. Lea el acuerdo de licencia y toque la casilla de verificación **Acepto el acuerdo de licencia**.
6. En la pantalla **Configura tu perfil**, toque **Configurar**. La configuración del perfil de trabajo puede tardar unos instantes.
7. Elija un método de desbloqueo de pantalla.
8. Si en la pantalla **Inicio seguro** se le solicita que requiera una contraseña cuando se inicie el dispositivo, toque **Sí**.
9. Escriba la contraseña del dispositivo, repítala para confirmarla y, después, toque **Aceptar**.
10. Seleccione cómo desea que se muestren sus notificaciones y, a continuación, toque **Listo**.
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 **Inscribir**.
13. Si desea configurar la autenticación de huella dactilar para las aplicaciones UEM Client y BlackBerry Dynamics, siga las instrucciones que aparecen en pantalla. De lo contrario, toque **Cancelar**.
14. Si se ha cerrado la sesión en su dispositivo, desbloquéelo para completar la activación de BlackBerry UEM.
15. Si se le solicita que permita la conexión a BlackBerry Secure Connect Plus, toque **Aceptar** y espere a que se active la conexión.
16. Si se le pide que instale aplicaciones de trabajo en su dispositivo, siga las instrucciones que aparecen en pantalla.

Después de terminar: Para verificar que el proceso de activación se haya 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 dispositivos iOS

Los pasos que siguen los usuarios para instalar BlackBerry UEM Client y activar los dispositivos iOS y iPadOS dependen de la versión del sistema operativo del dispositivo y de si el tipo de activación incluye controles MDM. Puede proporcionar instrucciones de activación del dispositivo en el correo electrónico de activación que envíe a los usuarios. Para obtener más información sobre la creación de una plantilla de correo electrónico de activación, consulte Creación de una plantilla de correo electrónico de activación.

Activar un dispositivo iOS o iPadOS con el tipo de activación de Controles de MDM

Para activar dispositivos con el tipo de activación Controles de MDM o el tipo de activación Privacidad del usuario con opciones de MDM activadas, envíe las siguientes instrucciones de activación a los usuarios del dispositivo.

Durante la activación, los usuarios deben salir de la aplicación BlackBerry UEM Client para instalar manualmente el perfil de MDM.

Antes de empezar: Si el modo de bloqueo está activado en el dispositivo (iOS y iPadOS 16 o posterior), debe desactivarlo para activar el dispositivo. El modo de bloqueo impide la instalación de los perfiles de configuración necesarios para la activación. Si es necesario, puede activar el modo de bloqueo después de la activación.

1. En su dispositivo, instale UEM Client desde App Store.
2. Abra el UEM Client y acepte el contrato de licencia.
3. Lleve a cabo una de estas acciones:

Tarea	Pasos
Escanee 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 en el correo electrónico de activación que ha recibido.
Active manualmente el dispositivo.	**a.** Escriba la dirección de correo electrónico del trabajo y la contraseña de activación. **b.** Si es necesario, escriba la dirección del servidor. Puede encontrar la dirección del servidor en el correo electrónico de activación que ha recibido o en BlackBerry UEM Self-Service. **c.** Toque **Siguiente**.

4. Toque **Permitir** para permitir que el UEM Client le envíe notificaciones. Si selecciona **No permitir**, el dispositivo no se podrá activar.
5. Cuando se le solicite instalar un perfil de configuración, toque **Aceptar**.
6. Cuando se le solicite descargar el perfil de configuración, toque **Permitir**.
7. Cuando haya finalizado la descarga, abra **Configuración**.
8. Toque **General** y vaya a **VPN y administración de dispositivos**.
9. Para instalar el perfil, toque **Perfil de BlackBerry UEM** y siga las instrucciones que aparecen en pantalla.
10. Cuando haya concluido la instalación, vuelva a la aplicación UEM Client para completar la activación.

11. Si se le pide que instale aplicaciones de trabajo en su dispositivo, siga las instrucciones que aparecen en pantalla.

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

- En el dispositivo, abra UEM Client y toque **Acerca de**. En las secciones **Dispositivo activado** y **Estado de conformidad**, compruebe que la información del dispositivo y la marca de tiempo de activación están presentes.
- En BlackBerry UEM Self-Service, compruebe que el dispositivo aparezca como un dispositivo activado. El estado puede tardar hasta dos minutos en actualizarse una vez que haya activado el dispositivo.

Activación de un dispositivo con iOS o iPadOS con la inscripción de usuario de Apple

La inscripción de usuarios de Apple es compatible con dispositivos que ejecuten versiones compatibles de iOS y iPadOS. Para activar los dispositivos con la inscripción de usuarios de Apple, envíe las siguientes instrucciones de activación a los usuarios de los dispositivos.

Antes de empezar:

- Verifique que ha recibido un correo electrónico de activación con un QR Code para la inscripción de usuario de Apple. Si no ha recibido el correo electrónico, póngase en contacto con un administrador.
- Si su dispositivo ya está activado con BlackBerry UEM, debe desactivarlo.
- Desinstale BlackBerry UEM Client.
- Debe tener una cuenta de Apple ID gestionada a través de su empresa.
- Su dispositivo no debe estar supervisado. Si su dispositivo está supervisado, se indicará en la aplicación Configuración, junto a su ID de Apple.
- Si el modo de bloqueo está activado en el dispositivo (iOS y iPadOS 16 o posterior), debe desactivarlo para activar el dispositivo. El modo de bloqueo impide la instalación de los perfiles de configuración necesarios para la activación. Si es necesario, puede activar el modo de bloqueo después de la activación.

1. Abra el correo electrónico de activación que contiene el QR Code para la inscripción de usuario de Apple. Si el QR Code ha caducado, puede solicitar un nuevo código de activación desde BlackBerry UEM Self-Service o ponerse en contacto con su administrador.
2. En su dispositivo, abra la aplicación de la cámara y escanee el código QR del correo electrónico de activación. Cuando se le solicite, toque la notificación para abrir la URL en Safari.
3. Cuando se le solicite descargar el perfil de configuración de UEM, toque **Permitir**.
4. Cuando finalice la descarga, toque **Cerrar**.
5. Vaya a **Configuración > General > Perfil**.
6. Toque **Perfil de UEM**.
7. En la pantalla de inscripción de usuario, toque **Inscribir mi iPhone** o **Inscribir mi iPad**.
8. Introduzca su contraseña.
9. Inicie sesión en su cuenta de ID de Apple con sus credenciales de ID de Apple gestionadas.
10. Si su administrador le ha asignado UEM Client, toque en **Instalar** cuando se le solicite, o abra Work Apps.
11. Para configurar UEM Client, ábralo y acepte el acuerdo de licencia. Siga las instrucciones que aparecen en pantalla para completar el proceso de activación.

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

- En el dispositivo, abra UEM Client y toque **Acerca de**. En las secciones **Dispositivo activado** y **Estado de conformidad**, compruebe que la información del dispositivo y la marca de tiempo de activación están presentes.
- En BlackBerry UEM Self-Service, compruebe que el dispositivo aparezca como un dispositivo activado. El estado puede tardar hasta dos minutos en actualizarse una vez que haya activado el dispositivo.

Activación de un dispositivo con macOS o Apple TV con BlackBerry UEM Self-Service

Los usuarios activan los dispositivos macOS y Apple TV mediante BlackBerry UEM Self-Service. Para obtener más información e instrucciones, consulte la Guía del usuario de UEM Self-Service.

Activación de una tableta o un equipo Windows 10

Para activar los dispositivos Windows 10, envíe las siguientes instrucciones de activación a los usuarios de los dispositivos. Tenga en cuenta que si desea gestionar los dispositivos Windows 10 con el tipo de activación Controles de MDM, los dispositivos no se pueden gestionar mediante Microsoft System Center Configuration Manager.

Envíe las instrucciones de activación siguientes al usuario del dispositivo.

Antes de empezar: Verifique que ha recibido un correo electrónico de activación con una dirección del servidor de certificados. Si no ha recibido el correo electrónico, póngase en contacto con su administrador.

1. En el navegador de su dispositivo, escriba o pegue la dirección del servidor de certificados.
2. Haga clic en **Guardar**.
3. En la notificación de descarga del certificado, haga clic en **Abrir**.
4. Haga clic en **Abrir**.
5. Haga clic en **Instalar certificado**.
6. Seleccione la opción **Usuario actual** y haga clic en **Siguiente**.
7. Seleccione la opción **Colocar todos los certificados en el siguiente almacén** y haga clic en **Examinar**.
8. Seleccione **Entidades de certificación raíz de confianza** y haga clic en **Aceptar**.
9. Haga clic en **Aceptar > Finalizar > Aceptar > Aceptar**.
10. Haga clic en el botón **Inicio**.
11. Lleve a cabo una de estas acciones:

Versión del SO del dispositivo	Pasos
Windows 10 versión 1607 o posterior	**a.** Toque **Configuración > Cuentas > Acceso de trabajo o escuela**. **b.** Toque **Inscribir solo en gestión de dispositivos**.
Windows 10 versión anterior a 1607	**a.** Toque **Configuración > Cuentas > Acceso de trabajo**. **b.** Toque **Conectarse**.

12. En el campo **Dirección de correo electrónico**, escriba su dirección de correo electrónico y toque **Continuar**.
13. Si se solicita, en el campo **Servidor**, escriba el nombre del servidor y toque **Continuar**. Puede encontrar el nombre del servidor en el correo de activación que ha recibido de su administrador o en BlackBerry UEM Self-Service cuando establece la contraseña de activación.
14. En el campo **Contraseña de activación**, escriba la contraseña de activación y toque **Continuar**. Puede encontrar la contraseña de activación en el correo electrónico de activación que ha recibido de su administrador o puede establecer su propia contraseña de activación en UEM Self-Service.
15. Toque **Hecho**.

Después de terminar:

- Para verificar que el proceso de activación se haya completado correctamente, realice una de las siguientes acciones:
  - En el dispositivo, haga clic en **Configuración > Cuentas > Acceso de trabajo o escuela** (o Acceso de trabajo) para confirmar que el dispositivo esté conectado a UEM.
  - En UEM Self-Service, compruebe que el dispositivo aparezca como un dispositivo activado. El estado puede tardar hasta dos minutos en actualizarse una vez que haya activado el dispositivo.
- Si se solicita por parte del administrador, agregue su cuenta de trabajo a Cuentas utilizadas por otras aplicaciones para que pueda acceder a las aplicaciones en línea necesarias.

- Para Windows 10 versión 1607 o posterior, haga clic en **Configuración > Cuentas > Acceso de trabajo y escuela > Conectar**. Escriba su dirección de correo de trabajo y contraseña.
- Para Windows 10 versión anterior a 1607, haga clic en **Configuración > Cuentas > Sus cuentas y correo electrónico**. En Cuentas utilizadas por otras aplicaciones, haga clic en Agregar una cuenta de trabajo o escuela y escriba la dirección de correo de trabajo y la contraseña.

Configuración de la compatibilidad con el aprovisionamiento automático de Android

Puede utilizar el aprovisionamiento automático de Android en BlackBerry UEM para implementar un gran número de dispositivos Android Enterprise a la vez. Los dispositivos deben ser compatibles con el aprovisionamiento automático.

Cuando su empresa adquiere dispositivos compatibles de un distribuidor autorizado, se configura una cuenta de aprovisionamiento automático y se añaden los dispositivos a la cuenta. Cuando los usuarios configuran uno de estos dispositivos por primera vez o restablecen los valores predeterminados de fábrica de un dispositivo, el dispositivo descarga BlackBerry UEM Client automáticamente e inicia el proceso de activación de UEM.

Tenga en cuenta que si el usuario reinicia el dispositivo antes de que finalice la activación, cancela la activación o permite que la batería se agote antes de que finalice la activación, el dispositivo se restablece automáticamente a los valores predeterminados de fábrica y el proceso de activación se reinicia.

1. En la barra de menús de la consola de administración, haga clic en **Configuración > Integración externa**.
2. Haga clic en **Android Enterprise**.
3. Haga clic en **Iniciar consola sin contacto**.
4. Si es la primera vez que se conecta al aprovisionamiento automático de Android con UEM, haga clic en **Siguiente** e inicie sesión en Google utilizando la dirección asociada a la cuenta de aprovisionamiento automático de su empresa.
5. Cree o gestione configuraciones de inscripción y asígnelas a los dispositivos.

   También puede utilizar el portal de aprovisionamiento automático de Android para gestionar las configuraciones de inscripción.

Después de terminar:

- En UEM, compruebe que los perfiles y las políticas de TI adecuados se han asignado a los usuarios. Para utilizar el aprovisionamiento automático, debe asignar un perfil de activación con el tipo de activación Trabajo y personal: control total (Android Enterprise) o Solo espacio de trabajo (Android Enterprise) activado.
- Distribuya los dispositivos a los usuarios.

Active varios dispositivos mediante Knox Mobile Enrollment

Puede utilizar Samsung Knox Mobile Enrollment para implementar un gran número de dispositivos Samsung Knox a la vez. Su empresa compra dispositivos a un distribuidor autorizado o a un distribuidor que esté dispuesto a compartir los IMEI de los dispositivos directamente con Samsung para que el dispositivo pueda utilizar Knox Mobile Enrollment. Cuando los usuarios configuran uno de estos dispositivos por primera vez o restablecen los valores predeterminados de fábrica de un dispositivo, el dispositivo descarga BlackBerry UEM Client automáticamente e inicia el proceso de activación de BlackBerry UEM.

Tenga en cuenta que si el usuario reinicia el dispositivo antes de que finalice la activación, cancela la activación o permite que la batería se agote antes de que finalice la activación, el dispositivo se restablece automáticamente a los valores predeterminados de fábrica y el proceso de activación se reinicia.

Nota: Knox Mobile Enrollment no es compatible con la inscripción basada en la administración de dispositivos en dispositivos con Android 11 o posterior. Para obtener más información, consulte Notas de la versión de KNOX Mobile Enrollment 1.36.

1. En la barra de menús de la consola de administración, haga clic en **Configuración > Integración externa > KNOX Mobile Enrollment**.
2. Descargue el archivo .json de UEM.
3. Siga los pasos que aparecen en pantalla.

Después de terminar: Una vez finalizada la activación, con el archivo JSON que ha descargado, compare la entrada de la sección CFPrint con la entrada que añadió al configurar Knox Mobile Enrollment. Si las entradas son diferentes, en el campo **Datos JSON personalizados** de la página Knox Mobile Enrollment, copie todo el texto del archivo .json.

Activación de los dispositivos iOS que están inscritos en DEP

Puede inscribir los dispositivos iOS y iPadOS en el Programa de inscripción de dispositivos (DEP) de Apple y asignar configuraciones de inscripción a los dispositivos mediante la consola de administración de BlackBerry UEM. Las configuraciones de inscripción incluyen reglas adicionales que se asignan a los dispositivos durante la inscripción de MDM.

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

Para activar los dispositivos inscritos en el DEP, realice las siguientes acciones:

Paso	Acción
1	Registrar los dispositivos iOS en DEP y asignarlos a un servidor BlackBerry UEM.
2	Adición de una configuración de inscripción DEP.
3	De forma opcional, para añadir BlackBerry UEM Client a la lista de aplicaciones y asignarlo a cuentas de usuario o grupos de usuarios, consulte Añadir una aplicación de iOS a la lista de aplicaciones.
4	Si no desea utilizar el perfil de activación predeterminado, cree un perfil de activación y asígnelo a dispositivos DEP (Usuarios > Dispositivos DEP de Apple).
5	Elija cómo desea que los usuarios activen sus dispositivos: • Envío de un mensaje de correo electrónico de activación a varios usuarios o envíe un correo electrónico de activación a un usuario específico mediante la plantilla de correo electrónico de DEP de Apple. • Si ha conectado UEM al directorio de la empresa, los usuarios pueden utilizar los nombres de usuario y las contraseñas del directorio de la empresa. Los usuarios deben introducir sus nombres de usuario en el formato dominio\nombredeusuario (las credenciales coinciden con las variables de dominio y nombre de usuario de su empresa ("%UserDomain%/%UserName%")). • Puede Asignación de un usuario a un dispositivo con iOS. Cuando asigna un usuario a un dispositivo en UEM, no se le solicita que introduzca un nombre de usuario o una contraseña durante la activación del dispositivo.
6	Distribuya dispositivos a los usuarios y solicite que completen la activación. Tras finalizar la activación, los usuarios deben instalar y abrir UEM Client.

Registrar los dispositivos iOS en DEP y asignarlos a un servidor BlackBerry UEM

Para registrar dispositivos iOS en el Programa de inscripción de dispositivos (DEP) de Apple, debe introducir los números de serie de los dispositivos en el portal de DEP o Apple Business Manager y asignar los dispositivos al servidor BlackBerry UEM. Para introducir los números de serie, puede teclear cada número, seleccionar el número de pedido que Apple asignó a los dispositivos cuando los adquirió o cargar un archivo .csv que contenga los números de serie.

Antes de empezar: Configure BlackBerry UEM para DEP.

1. Inicie sesión en Apple Business Manager o en el portal de DEP.
2. En la sección **Programa de inscripción de dispositivos**, haga clic en **Gestionar dispositivos**.
3. Para introducir los números de serie del dispositivo, siga los pasos que aparecen en pantalla.
4. Asigne los números de serie al servidor UEM.

Después de terminar: Adición de una configuración de inscripción DEP.

Adición de una configuración de inscripción DEP

Una configuración de inscripción le permite definir cómo se configuran los dispositivos que están inscritos en DEP cuando se activan en BlackBerry UEM. Puede crear tantas configuraciones de inscripción como necesite la empresa.

Antes de empezar: Registrar los dispositivos iOS en DEP y asignarlos a un servidor BlackBerry UEM.

1. En la barra de menús de la consola de administración, haga clic en **Configuración > Integración externa > Programa de inscripción de dispositivos de Apple**.
2. Haga clic en el nombre de una cuenta de DEP.
3. En la sección **Configuraciones de inscripción de DEP**, haga clic en +.
4. Escriba un nombre para la configuración.
5. Si desea que UEM asigne automáticamente la configuración de inscripción cuando los dispositivos DEP se sincronicen con UEM, seleccione la casilla de verificación **Asignar automáticamente todos los nuevos dispositivos a esta configuración**.

   UEM se sincroniza con Apple DEP a diario y siempre que se visualiza la página de dispositivos DEP de Apple. Solo puede asignar automáticamente una configuración de inscripción a los nuevos dispositivos DEP. Si ha creado previamente una configuración de inscripción con esta configuración, la configuración se elimina de la configuración anterior y se agrega a la nueva. Si previamente se creó una configuración de inscripción con esta configuración y se aplicó a los dispositivos, UEM no asigna la nueva configuración de inscripción.
6. Opcionalmente, escriba el nombre de un departamento y un número de teléfono de soporte para que se muestren en los dispositivos durante la instalación.
7. En la sección **Configuración del dispositivo**, seleccione una de las opciones siguientes:
   - **Permitir emparejamiento**: los usuarios pueden emparejar el dispositivo con un equipo.
   - **Obligatorio**: a los usuarios no se les solicita que acepten la configuración de inscripción.
   - **Permitir la eliminación del perfil de MDM**: los usuarios pueden desactivar los dispositivos.
   - **Espere hasta que el dispositivo esté configurado**: los usuarios no pueden cancelar la configuración del dispositivo hasta que la activación haya finalizado.
8. En la sección **Omitir durante la configuración**, seleccione los elementos que no desea incluir en la instalación del dispositivo:

Opción	Impacto, si se selecciona
Código de acceso	A los usuarios no se les solicita que creen un código de acceso del dispositivo.
Servicios de ubicación	Los servicios de ubicación están desactivados en el dispositivo.
Restaurar	Los usuarios no pueden restaurar datos desde un archivo de copia de seguridad.
Mover desde Android	Los datos no se pueden restaurar desde un dispositivo Android.
Apple ID	Se impide que los usuarios inicien sesión en Apple ID y iCloud.
Términos y condiciones	Los usuarios no ven los términos y condiciones de iOS.
Siri	Siri está desactivado en los dispositivos.
Diagnostics	La información de diagnóstico no se envía automáticamente desde el dispositivo durante la instalación.
Biométrico	Los usuarios no pueden configurar Touch ID.
Pago	Los usuarios no pueden configurar Apple Pay.
Zoom	Los usuarios no pueden configurar Zoom.
Configuración del botón Inicio	Los usuarios no pueden ajustar el clic del botón Inicio.
Tiempo de pantalla	La opción para configurar el tiempo de pantalla se omitirá durante la inscripción en DEP.
Actualización de software	Los usuarios no ven la pantalla de actualización de software obligatoria en el dispositivo.
iMessage y FaceTime	Los usuarios no ven las pantallas iMessage y FaceTime en el dispositivo.
Tono para mostrar	Los usuarios no verán la pantalla de Tono para mostrar en el dispositivo.
Privacidad	Los usuarios no verán la pantalla Privacidad en el dispositivo.
Integración	Los usuarios no verán la pantalla informativa de integración en el dispositivo.
Migración de Watch	Los usuarios no verán la pantalla de migración de Watch en el dispositivo.
Configuración SIM	Los usuarios no verán la pantalla para configurar un plan móvil en el dispositivo.

Opción	Impacto, si se selecciona
Migración de dispositivo a dispositivo	Los usuarios no verán la pantalla de migración de dispositivo a dispositivo en el dispositivo.

9. Haga clic en **Guardar**. Si ha seleccionado la casilla de verificación **Asignar automáticamente los nuevos dispositivos a esta configuración**, haga clic en **Sí**.

Después de terminar:

- Si no ha seleccionado la casilla de verificación **Asignar automáticamente los nuevos dispositivos a esta configuración**, debe asignar la configuración de inscripción adecuada a los dispositivos. En **Usuarios > Dispositivos de Apple DEP**, seleccione los dispositivos registrados en la misma cuenta DEP y haga clic en . Seleccione la configuración de inscripción y asígnela.
- Si no desea utilizar el perfil de activación predeterminado, cree un perfil de activación y asígnelo a los dispositivos registrados en Apple DEP. En **Usuarios > Dispositivos de Apple DEP**, seleccione los dispositivos registrados en la misma cuenta DEP y haga clic en . Seleccione el perfil y asígnelo.
- Durante la activación del dispositivo, es posible que se solicite a los usuarios un nombre de usuario y una contraseña. Elija cómo desea que los usuarios activen sus dispositivos:
  - Envío de un mensaje de correo electrónico de activación a varios usuarios o envíe un correo electrónico de activación a un usuario específico mediante la plantilla de correo electrónico de DEP de Apple.
  - Si ha conectado UEM al directorio de la empresa, los usuarios pueden utilizar los nombres de usuario y las contraseñas del directorio de la empresa. Los usuarios deben introducir sus nombres de usuario en el formato dominio\nombredeusuario (las credenciales coinciden con las variables de dominio y nombre de usuario de su empresa ("%UserDomain%/%UserName%")).
  - Puede Asignación de un usuario a un dispositivo con iOS. Cuando asigna un usuario a un dispositivo en UEM, no se le solicita que introduzca un nombre de usuario o una contraseña durante la activación del dispositivo.
- Distribuya dispositivos a los usuarios y solicite que completen la activación. Tras finalizar la activación, los usuarios deben instalar y abrir BlackBerry UEM Client.

Asignación de un usuario a un dispositivo con iOS

Puede asignar un usuario directamente a un dispositivo registrado en Apple DEP antes de que se active el dispositivo. Cuando asigna un usuario directamente al dispositivo, no se les solicita que introduzcan un nombre de usuario o una contraseña durante la activación del dispositivo.

1. En la barra de menús, haga clic en **Usuarios > Dispositivos de Apple DEP**.
2. En la columna **Asociación de usuario** del dispositivo que quiere asignar, haga clic en **Seleccionar**.
3. En el cuadro de búsqueda **Seleccionar usuario**, busque el usuario que desea asignar al dispositivo.
4. En la lista de resultados de la búsqueda, haga clic en la cuenta de usuario.
5. Haga clic en **Guardar**.

Después de terminar:

- Para ver el propietario de un dispositivo activado, en la columna **Asociación de usuarios**, haga clic en el enlace del nombre de usuario.
- Para eliminar un usuario de un dispositivo iOS, en la columna **Asociación de usuarios**, haga clic en el enlace del nombre de usuario del dispositivo del que desea eliminar el usuario. Haga clic en **Anular asignación**.

Activación de dispositivos iOS mediante Apple Configurator 2

Si tiene BlackBerry UEM en un entorno local, puede utilizar Apple Configurator 2 para preparar los dispositivos iOS y iPadOS para la activación. Los usuarios pueden activar dispositivos preparados sin utilizar BlackBerry UEM Client. Los usuarios solo necesitan su nombre de usuario y su contraseña de activación.

Apple Configurator no es compatible con UEM Cloud.

Nota: Algunas funciones de UEM requieren que asigne el UEM Client a los usuarios. Los usuarios deben iniciar UEM Client después de activar el dispositivo. Para obtener más información, consulte KB 39313.

Para activar los dispositivos iOS mediante Apple Configurator 2, realice las siguientes acciones:

Paso	Acción
1	También puede agregar UEM Client a la lista de aplicaciones y asignarlo a las cuentas de usuarios o a los grupos de usuarios. Consulte Adición de una aplicación de iOS a la lista de aplicaciones.
2	Adición de información del servidor de BlackBerry UEM a Apple Configurator 2.
3	Preparación de dispositivos iOS con Apple Configurator 2.
4	Cree un perfil de activación y asígnelo a una cuenta de usuario o a un grupo de usuarios.
5	Envío de un mensaje de correo electrónico de activación a varios usuarios O envíe un mensaje de correo electrónico de activación a un usuario específico.
6	Distribuya dispositivos a los usuarios y solicite que completen la activación. Para aplicar un perfil de conformidad, los usuarios deben instalar y abrir la aplicación UEM Client una vez finalizada la activación.

Adición de información del servidor de BlackBerry UEM a Apple Configurator 2

Antes de empezar: Descargue e instale la última versión de Apple Configurator 2 de Apple.

1. En el menú de Apple Configurator 2, seleccione **Preferencias > Servidores**.
2. Haga clic en + > **Siguiente**.
3. En el campo **Nombre**, escriba un nombre para el servidor.
4. En el campo **Nombre de host o URL**, escriba la URL del servidor de UEM con el formato *<http or https>://<servername>:<port>*, donde el número de puerto predeterminado es 8885.
5. Haga clic en **Siguiente**.
6. Cierre la ventana **Servidor**.

Después de terminar: Preparación de dispositivos iOS con Apple Configurator 2.

Preparación de dispositivos iOS con Apple Configurator 2

Cuando prepare un dispositivo, Apple Configurator 2 borra el dispositivo y actualiza el sistema operativo del dispositivo a la versión más reciente.

Antes de empezar: Adición de información del servidor de BlackBerry UEM a Apple Configurator 2.

1. Abra Apple Configurator 2.
2. Conecte uno o más dispositivos iOS al equipo.
3. Haga clic en **Preparar**.
4. En la lista desplegable **Configuración**, seleccione **Manual**. Haga clic en **Siguiente**.
5. En la lista desplegable **Servidor**, seleccione el servidor de BlackBerry UEM. Haga clic en **Siguiente**.
6. De manera opcional, seleccione la casilla de verificación **Supervisar dispositivos**. Haga clic en **Siguiente**.
7. Si selecciona **Supervisar dispositivos**, complete la información de la empresa.
8. Haga clic en **Preparar** y espere a que el dispositivo esté preparado. El proceso puede tardar hasta 15 minutos.

Después de terminar: Distribuya los dispositivos a los usuarios para la activación.

Importación o exportación de una lista de ID de los dispositivos aprobados

Puede importar y exportar una lista de identificadores de dispositivo únicos para limitar los dispositivos que puedan inscribirse con BlackBerry UEM. Actualmente, el único identificador único que admite UEM es el número de serie del dispositivo.

Antes de empezar: Para importar una lista, asegúrese de que dispone de un archivo .csv que contenga una lista de identificadores de dispositivo únicos.

1. En la barra de menús de la consola de administración, haga clic en **Configuración > Configuración general > Valores predeterminados de activación**.
2. En la sección **Importar o exportar ID de los dispositivos**, junto al campo **Cargar ID de los dispositivos aprobados (.csv)**, haga clic en **Examinar**.
3. Desplácese hasta el archivo .csv.
4. Haga clic en **Abrir**.
5. Haga clic en **Guardar**.

Después de terminar: Para exportar la lista, haga clic en **Exportar ID de los dispositivos aprobados (.csv)**.

Desactivación de dispositivos

Cuando se desactiva un dispositivo, se elimina la conexión entre el dispositivo y la cuenta de usuario en BlackBerry UEM. 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.

Un dispositivo puede desactivarse utilizando cualquiera de los siguientes métodos:

- Los administradores pueden desactivar un dispositivo desde la consola de administración de UEM mediante el comando "Eliminar solo los datos de trabajo" o "Eliminar todos los datos del dispositivo".
- UEM puede desactivar un dispositivo si infringe las normas del perfil de conformidad asignado y la acción de cumplimiento configurada es desactivar el dispositivo.
- Los usuarios pueden desactivar un dispositivo desde UEM Self-Service mediante el comando "Eliminar solo los datos de trabajo" o "Eliminar todos los datos del dispositivo".
- Los usuarios pueden utilizar UEM Client para desactivar los dispositivos iOS y Android.
- Los usuarios pueden desactivar los dispositivos Windows 10 en Configuración > Cuentas > Acceso de trabajo > Eliminar.

Tenga en cuenta las siguientes consideraciones al desactivar dispositivos con los tipos de activación especificados:

Tipo de activación	Consideraciones
Dispositivos Android Enterprise solo con perfil de trabajo	Tiene la opción de eliminar todos los datos de la tarjeta SD y la protección contra el restablecimiento de los datos de fábrica.
Dispositivos Android Enterprise con activaciones de Trabajo y personal: control total	• El comando "Eliminar todos los datos del dispositivo" solo es compatible con Android 10. UEM dejará de ser compatible con Android 10 a partir de enero de 2024. • El comando "Eliminar solo los datos de trabajo" es compatible con dispositivos Android 11 y versiones posteriores. Este comando elimina todos los datos de trabajo y aplicaciones, pero permite al usuario conservar los datos y las aplicaciones personales y seguir utilizando el dispositivo no gestionado.
Dispositivos Android Enterprise con Trabajo y personal: privacidad de usuario y activaciones de Trabajo y personal: control total	Si utiliza el comando "Eliminar solo los datos de trabajo", puede especificar un motivo que aparecerá en la notificación del dispositivo del usuario. Si el dispositivo se desactiva por infringir las normas de cumplimiento, la notificación especifica el motivo por el cual el dispositivo no cumplía con los requisitos de cumplimiento.
Knox MDM	• Las aplicaciones internas se desinstalan. • La opción de desinstalación pasa a estar disponible para cualquiera de las aplicaciones públicas que se instalaron de la lista de aplicaciones según se necesite.
Dispositivos con Samsung Knox Workspace con Trabajo y personal: control total	Al desactivar el dispositivo, se eliminan todos los datos de este. Puede especificar los datos que se borran utilizando la regla de política de TI "Borrado de datos durante la desactivación".

Resolución de problemas de activación del dispositivo

Siempre que solucione problemas de activación para cualquier tipo de dispositivo, compruebe lo siguiente:

- Compruebe que las licencias estén disponibles para el tipo de dispositivo y el tipo de activación.
- Compruebe que el perfil de activación asignado al dispositivo sea compatible con el tipo de dispositivo.
- Compruebe la conectividad de red en el dispositivo.
  - Verifique que el móvil o la red Wi-Fi esté activa y tenga cobertura suficiente.
  - Si se trata de la Wi-Fi de trabajo, asegúrese de que la ruta de red del dispositivo esté disponible.
  - Si el usuario debe configurar manualmente una VPN o un perfil de Wi-Fi de trabajo para acceder a contenido protegido por el firewall de la empresa, asegúrese de que los perfiles de usuario estén configurados correctamente en el dispositivo.
- Si ha configurado reglas de conformidad para dispositivos con sistemas con jailbreak o rooting, versiones de sistemas operativos restringidas o modelos de dispositivo restringidos, verifique que el dispositivo cumpla con los requisitos.
- Si UEM se instala en un entorno local y el dispositivo intenta conectarse con UEM o BlackBerry Infrastructure a través del firewall de su empresa, compruebe que los puertos correctos del firewall están abiertos.
- Recopilar registros del dispositivo. Para obtener más información sobre la recuperación de registros del dispositivo, consulte KB 36986 para iOS y KB 32516 para Android.

Dispositivos Android Management

- Debe crear perfiles de activación independientes para Android Enterprise y Android Management. Si se especifican tipos de activación Android Enterprise y Android Management en el mismo perfil, el tipo Android Management tendrá prioridad aunque esté clasificado por debajo de Android Enterprise. Solo la contraseña y la información de activación del tipo de activación Android Management se incrustarán en el código QR.
- En algunos dispositivos, es posible que aparezca una pantalla innecesaria "Configuración y restauración" después de que el dispositivo complete correctamente el proceso de activación.

Dispositivos Knox Workspace y Android Enterprise

Cuando solucione problemas de activación de dispositivos Samsung que utilizan Samsung Knox Workspace, compruebe que la versión del contenedor Knox sea compatible. Knox Workspace requiere Knox Container 2.0 o una versión posterior.

Cuando solucione problemas de activación de dispositivos Android Enterprise, compruebe que la cuenta de usuario UEM tenga la misma dirección de correo electrónico que en el dominio Google. Si las direcciones de correo electrónico no coinciden, el dispositivo mostrará el error "No se puede activar el dispositivo - Tipo de activación no compatible".

Solución de problemas: errores y problemas de activación

Errores de activación

Error	Solución posible
No se puede completar la activación del dispositivo porque el servidor no tiene más licencias. Para obtener ayuda, contacte con el administrador.	En la consola de administración de UEM, compruebe que las licencias estén disponibles. Si es necesario, active las licencias o adquiera licencias adicionales.
Error de instalación del perfil. No se ha podido importar el certificado "AutoMDMCert.pfx".	Este error se muestra en un dispositivo iOS cuando ya existe un perfil en el dispositivo. Vaya a **Configuración > General > Perfiles** en el dispositivo y compruebe que el perfil ya existe. Elimine el perfil e intente activarlo de nuevo. Si el problema persiste, es posible que tenga que reiniciar el dispositivo porque los datos podrían almacenarse en la memoria caché.
Error en el perfil de instalación: la nueva carga de MDM no coincide con la antigua.	Este error se muestra en un dispositivo iOS cuando ya existe un perfil en el dispositivo. Vaya a **Configuración > General > Perfiles** en el dispositivo y compruebe que el perfil ya existe. Elimine el perfil e intente activarlo de nuevo. Si el problema persiste, es posible que tenga que reiniciar el dispositivo porque los datos podrían almacenarse en la memoria caché.
Error 3007: el servidor no está disponible.	Este error puede producirse si el certificado que utiliza UEM para firmar el perfil de MDM que envía a un dispositivo iOS no es de confianza para el dispositivo (se solicita al usuario que confíe en este certificado cuando activa el dispositivo). En un entorno local, instale el certificado raíz de la CA que emitió el certificado. Consulte Modificación de los certificados que BlackBerry UEM utiliza para la autenticación en el contenido de Configuración. Este error también puede producirse si configura un proxy transparente, como Blue Coat, que supervise el puerto 443 para el tráfico no estándar y el UEM Client no puede realizar las llamadas HTTP CONNECT y HTTP OPTIONS necesarias al UEM. Compruebe que la configuración del proxy no impida que UEM Client realice estas llamadas.
No se ha podido establecer la conexión con el servidor; compruebe la conectividad o la dirección del servidor.	Este error puede producirse si el nombre de usuario (o la dirección del cliente si el registro con el BlackBerry Infrastructure estaba desactivado) no se ha introducido correctamente o si la contraseña de activación no se ha establecido o ha caducado. Compruebe que el nombre de usuario, la contraseña y la dirección del cliente (si procede) sean correctos o establezca una nueva contraseña de activación con UEM Self-Service e inténtelo de nuevo.

Problemas de activación

Problema	Solución posible
Las activaciones de dispositivos iOS o macOS dan error con un certificado APN no válido.	Es posible que el certificado APN no esté registrado correctamente. Realice una o más de las acciones siguientes: • En la barra de menús de la consola de administración, haga clic en **Configuración > Integración externa > Apple Push Notification**. Compruebe que el estado del certificado APN sea "Instalado". Si el estado no es correcto, intente registrar el certificado APN de nuevo. • Para probar la conexión entre UEM y el servidor de APN, haga clic en **Probar certificado APN**. • Si es necesario, obtenga una nueva CSR firmada de BlackBerry y solicite y registre un nuevo certificado APN. Para obtener más información, consulte Adquisición de un certificado APN para gestionar dispositivos iOS y macOS en el contenido de Configuración.
Los usuarios no reciben el correo electrónico de activación.	Si los usuarios utilizan un servidor de correo de terceros, los mensajes de correo procedentes de UEM se pueden marcar como no deseados y terminar en la carpeta de correo no deseado.
La pantalla de detalles de usuario de UEM muestra más dispositivos Windows activados de los esperados.	Cuando un usuario instala BlackBerry Access y BlackBerry Work para Windows en un equipo, estas aplicaciones se muestran como un dispositivo Windows en la pantalla de detalles del usuario. Este es el comportamiento esperado.

Aviso legal

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

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

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

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

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

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

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

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

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

Publicado en Canadá