BlackBerry UEM

Administrar dispositivos iOS y macOS

12.17

Contents

Gestión de dispositivos iOS y iPadOS

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

Apple presentó iPadOS como un sistema operativo independiente a partir de iPadOS 13. Debido a las grandes similitudes entre iOS y iPadOS, casi todas las características y documentación de BlackBerry UEM que se aplican a iOS también se aplican a iPadOS.

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

Administración de otros dispositivos Apple

También puede activar y administrar dispositivos macOS y Apple TV en BlackBerry UEM. Apple TV es un reproductor multimedia digital que puede recibir datos y transferirlos a un televisor a través de un cable HDMI.

BlackBerry UEM es compatible con las versiones de Apple TV de segunda generación o posteriores. Para obtener más información sobre las versiones de macOS compatibles, consulte las matrices de compatibilidad. Para gestionar los dispositivos Apple TV, siga las instrucciones y utilice los ajustes del perfil para los dispositivos iOS. Las siguientes funciones de BlackBerry UEM son compatibles con Apple TV:

- Activación del dispositivo mediante BlackBerry UEM Self-Service
- Tipo de activación de los controles MDM
- Wi-Fi y perfiles de certificado
- Perfiles de modo de bloqueo de la aplicación
- Comandos del dispositivo

Para evitar que los usuarios activen dispositivos Apple TV, establezca la restricción de modelo de dispositivo en el perfil de activación para no permitir dispositivos Apple TV. Para obtener más información sobre la activación de dispositivos macOS y Apple TV, consulte el contenido referente a la activación de dispositivos.

Lo que puede controlar en los dispositivos con iOS

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

Nivel de control	Descripción
Dispositivos sin administrar o parcialmente administrados (dispositivos activados en BlackBerry UEM, pero no administrados del todo)	Puede activar un dispositivo en BlackBerry UEM para proporcionar un acceso seguro a los recursos de trabajo sin administrar el dispositivo. Esta opción suele utilizarse para dispositivos BYOD. Estas activaciones pueden permitir que el usuario acceda a su red a través de VPN mediante BlackBerry 2FA, compartir archivos de forma segura con BlackBerry Workspaces, e instalar aplicaciones BlackBerry Dynamics como BlackBerry Work y BlackBerry Access para acceder al correo de trabajo y a su intranet de trabajo.
Dispositivos gestionados parcialmente con un perfil de trabajo	Puede activar un dispositivo en BlackBerry UEM para proporcionar un acceso seguro a los recursos de trabajo en un perfil de trabajo. Esta opción suele utilizarse para dispositivos BYOD. Con este tipo de activación, se crea 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 (adjuntos) y iCloud Keychain nativas.
Dispositivos administrados (dispositivos administrados por BlackBerry UEM)	Puede activar un dispositivo para administrarlo en su totalidad mediante BlackBerry UEM. Esta opción suele utilizarse en los dispositivos de propiedad corporativa. Esta opción le permite administrar los datos de trabajo mediante el uso de comandos y reglas de políticas de TI. Puede administrar las aplicaciones de trabajo de un dispositivo, incluidas las aplicaciones BlackBerry Dynamics. BlackBerry UEM es compatible con la administración de dispositivos con iOS supervisados. Ciertas reglas de políticas de TI solo son compatibles con dispositivos supervisados

Las **Activaciones de la privacidad del usuario** pueden proporcionar capacidades de administración de dispositivos limitadas y permitir que los usuarios accedan a los datos de trabajo a través de aplicaciones BlackBerry Dynamics, como BlackBerry Work y BlackBerry Access. Puede optar por permitir ciertas de las siguientes funciones de administración de dispositivos:

- Acceso a la tarjeta SIM y a la información de hardware del dispositivo: permitir que BlackBerry UEM acceda a la tarjeta SIM y a la información del hardware del dispositivo para activar licencias basadas en SIM.
- Administración de aplicaciones: permitir que los administradores instalen o eliminen aplicaciones de trabajo y mostrar una lista con las aplicaciones de trabajo instaladas en la pantalla de detalles del usuario.
- Administración de políticas de TI: permitir que se aplique un conjunto limitado 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).
- Administración de perfiles de correo electrónico: permitir que se apliquen perfiles de correo electrónico al dispositivo.
- Administración de perfiles de Wi-Fi: permitir que se apliquen perfiles de Wi-Fi al dispositivo.

- Administración de perfiles VPN: permitir que se apliquen perfiles VPN al dispositivo.

Las **activaciones de Privacidad de usuario: inscripción de usuario** mantienen los datos de usuario privados y separados de los datos de trabajo. Con este tipo de activación, se instala un espacio de trabajo independiente en el dispositivo para las aplicaciones de trabajo y algunas aplicaciones 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 no supervisados con iOS o iPadOS 13.1 o posterior.

Las **activaciones de Controles de MDM** proporcionan una compatibilidad completa para administrar dispositivos con iOS, con la inclusión de las siguientes funciones:

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

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

Pasos para administrar dispositivos con iOS

Paso	Acción
1	Instale y configure BlackBerry UEM según las instrucciones de instalación locales o las UEM Cloud instrucciones de configuración. Para administrar dispositivos con iOS y iPadOS, debe obtener un certificado de APN de Apple.
2	Si su empresa utiliza el programa de inscripción de dispositivos de Apple, configure BlackBerry UEM para utilizar DEP.
3	Configure las políticas de TI para dispositivos. Asigne políticas de TI a grupos de usuarios o usuarios individuales.
4	Configure perfiles para dispositivos. Asigne perfiles a grupos de usuarios o usuarios individuales.
5	Si su empresa tiene una cuenta VPP de Apple, agréguela a BlackBerry UEM.
6	Especifique las aplicaciones que los dispositivos pueden o deben instalar.
7	Active los dispositivos.
8	Administre y controle los dispositivos.

Control de dispositivos con una política de TI

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

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

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

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

- Requisitos de contraseñas del dispositivo
- Permitir funciones del dispositivo, como la cámara, el Bluetooth y Touch ID
- Permitir compras en App Store y iTunes Store, así como clasificaciones de contenido permitido para compras
- Permitir aplicaciones del sistema, como Safari, Siri y FaceTime
- Permitir el uso de iCloud

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

Establecimiento de los requisitos de la contraseña de iOS

Puede elegir si los dispositivos iOS y iPadOS deben tener una contraseña. Si se requiere una contraseña, puede establecer los requisitos para esta.

Nota: Los dispositivos iOS y iPadOS y algunas reglas para la contraseña del dispositivo utilizan el término "código de acceso". Ambos, tanto "contraseña" como "código de acceso", tienen el mismo significado.

Regla	Descripción
Se requiere contraseña para el dispositivo	Especifique si el usuario debe establecer una contraseña para el dispositivo.
Permitir valor simple	Especifique si la contraseña puede contener caracteres repetidos o secuenciales, como DEFG o 3333.
Requerir valor alfanumérico	Especifique si la contraseña deberá contener letras y números.
Longitud mínima del código	Especifique la longitud mínima de la contraseña. Si introduce un valor que es menor que el mínimo requerido por el dispositivo, se utiliza dicho mínimo.
Número mínimo de caracteres complejos	Especifique el número mínimo de caracteres no alfanuméricos que debe contener la contraseña del dispositivo.

Regla	Descripción
Periodo máximo de validez del código	Especifique el número máximo de días que puede utilizarse la contraseña.
Bloqueo automático máximo	Especifique el valor máximo que un usuario puede establecer para el tiempo de bloqueo automático, que se corresponde con el número de minutos de inactividad del usuario que deben transcurrir antes de que el dispositivo se bloquee. Si se establece en "Ninguno", todos los valores compatibles estarán disponibles en el dispositivo. Si el valor seleccionado se encuentra fuera del intervalo compatible con el dispositivo, el dispositivo utilizará el valor más cercano compatible.
Historial de códigos	Especifique el número de contraseñas anteriores que el dispositivo debe comprobar para evitar que un usuario vuelva a utilizar una contraseña reciente.
Periodo máximo de gracia para el bloqueo del dispositivo	Especifique el valor máximo que un usuario puede establecer para el periodo de gracia para el bloqueo del dispositivo, que se corresponde con la cantidad de tiempo que un dispositivo puede permanecer bloqueado antes de que se requiera una contraseña para desbloquearlo. Si se establece en "Ninguno", todos los valores estarán disponibles en el dispositivo. Si se establece en "Inmediatamente", la contraseña se necesita inmediatamente después de que el dispositivo se bloquee.
Número máximo de intentos de contraseña fallidos	Especifique el número de veces que un usuario puede introducir una contraseña incorrecta antes de que se eliminen los datos del dispositivo.
Permitir cambios de contraseñas (solo con supervisión)	Especifique si un usuario puede agregar, cambiar o eliminar la contraseña.

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

Control de dispositivos con perfiles

BlackBerry UEM incluye varios modos que puede utilizar para controlar diversos aspectos de la funcionalidad de los dispositivos con iOS y iPadOS. Entre los más utilizados, se incluyen los siguientes perfiles:

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

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

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

Referencia de perfiles: dispositivos iOS

La siguiente tabla enumera todos los perfiles de BlackBerry UEM compatibles con dispositivos iOS y iPadOS:

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

Nombre de perfil	Descripción	Configurar
Conformidad (BlackBerry Dynamics)	Este es un perfil de solo lectura que muestra los ajustes de conformidad importados de Good Control a BlackBerry UEM local.	Gestión de perfiles de conformidad de BlackBerry Dynamics
Correo, calendario y contactos		
Correo	Especifica cómo se conectan los dispositivos al servidor de correo de trabajo y cómo sincronizan los mensajes de correo, las entradas del calendario y los datos del organizador mediante Exchange ActiveSync o IBM Notes Traveler.	Crear un perfil de correo electrónico
IMAP/correo electrónico POP3	Especifica la forma de conexión de los dispositivos a un servidor de correo electrónico IMAP o POP3 y cómo sincronizar mensajes de correo electrónico.	Creación de un perfil de correo IMAP/POP3
Enlace	Especifica los servidores de Microsoft Exchange que se deben utilizar para un enlace automático.	Creación de un perfil de enlace
CalDAV	Especifica los ajustes del servidor que los dispositivos pueden utilizar para sincronizar la información del calendario.	Creación de un perfil de CalDAV
CardDAV	Especifica los ajustes del servidor que los dispositivos pueden utilizar para sincronizar la información de contacto.	Creación de un perfil de CardDAV
Redes y conexiones		
Wi-Fi	Especifica la forma de conexión de los dispositivos a una red Wi-Fi de trabajo.	Creación de un perfil de Wi-Fi
VPN	Especifica la forma de conexión de los dispositivos a una red VPN de trabajo.	Crear un perfil VPN
Proxy	Especifica cómo pueden usar un servidor proxy los dispositivos para acceder a servicios web en Internet o en una red de trabajo.	Creación de un perfil de proxy
Conectividad de la empresa	Especifica si los dispositivos pueden utilizar BlackBerry Secure Connect Plus.	Activar BlackBerry Secure Connect Plus
Conectividad de BlackBerry Dynamics	Define las conexiones de red, los dominios de Internet, los rangos de dirección IP y los servidores de aplicaciones a los que los dispositivos se pueden conectar cuando se usan aplicaciones de BlackBerry Dynamics.	Creación de un perfil de conectividad de BlackBerry Dynamics

Nombre de perfil	Descripción	Configurar
BlackBerry 2FA	Permite la autenticación de dos factores para los usuarios y especifica la configuración de las funciones de autenticación previa y de autorrescate.	Crear un perfil de BlackBerry 2FA
Uso de red	Permite controlar si las aplicaciones de trabajo pueden utilizar la red móvil o el roaming de datos.	Creación de un perfil de uso de red
Filtro de contenido web	Limita los sitios web que un usuario puede ver en dispositivos supervisados. Solo en dispositivos supervisados.	Creación de un perfil de filtro de contenido web
Extensión de registro único	Permite que los dispositivos se autentiquen mediante el inicio de sesión único.	Creación de un perfil de extensión de registro único
Dominios gestionados	Configura dispositivos para notificar a los usuarios sobre el envío de correo fuera de los dominios de confianza y restringe las aplicaciones que pueden ver los documentos descargados desde los dominios internos.	Creación de un perfil de dominios gestionados
AirPrint	Le permite agregar impresoras AirPrint a la lista de impresoras AirPrint de los usuarios.	Creación de un perfil de AirPrint
AirPlay	Le permite agregar dispositivos a la lista de dispositivos AirPlay de los usuarios.	Creación de un perfil de AirPlay
Protección		
Protección de aplicaciones de Microsoft Intune	Le permite gestionar las aplicaciones protegidas por Microsoft Intune.	Creación de un perfil de protección de aplicación de Microsoft Intune
Servicio de ubicación	Le permite solicitar la ubicación de los dispositivos y ver las ubicaciones aproximadas en un mapa.	Creación de un perfil de servicio de ubicación
No molestar	Le permite bloquear las notificaciones de BlackBerry Work for iOS durante los días fuera del trabajo que defina.	Crear un perfil de no molestar
Personalizada		
Dispositivo	Permite configurar la información que aparece en los dispositivos.	Creación de un perfil de dispositivo
Cargas personalizadas	Especifica la información de las configuraciones personalizadas que utiliza código de carga para los dispositivos.	Creación de un perfil de carga personalizado

Nombre de perfil	Descripción	Configurar
Notificación por aplicación	Le permite configurar los ajustes de notificación para las aplicaciones del sistema y las aplicaciones que gestiona mediante BlackBerry UEM. Solo en dispositivos supervisados.	Crear perfil de notificación por aplicación
Certificados		
Certificado de CA	Especifica un certificado de CA que los dispositivos pueden utilizar para establecer una conexión de confianza con una red o servidor de trabajo.	Creación de un perfil de certificado de CA
Certificado compartido	Especifica un certificado de cliente que los dispositivos puedan utilizar para autenticar usuarios en una red o servidor de trabajo.	Creación de un perfil de certificado compartido
Credencial de usuario	Especifica la conexión de CA que los dispositivos pueden utilizar para obtener un certificado de cliente utilizado para autenticar con una red o servidor de trabajo.	Creación de un perfil de credenciales de usuario
SCEP	Especifica el servidor SCEP que los dispositivos pueden utilizar para obtener un certificado de cliente utilizado para autenticar con una red o servidor de trabajo.	Crear un perfil SCEP

Administración de aplicaciones en dispositivos

Puede crear una biblioteca de aplicaciones que desee administrar y supervisar en los dispositivos. BlackBerry UEM proporciona las siguientes opciones para gestionar las aplicaciones en los dispositivos con iOS y iPadOS:

- Asignar aplicaciones públicas desde la App Store según sea obligatorio u opcional en los dispositivos.
- Cargar aplicaciones personalizadas a UEM e implementarlas como aplicaciones opcionales u obligatorias.
- Preconfigurar la configuración de las aplicaciones, como la configuración de conexión, cuando la aplicación lo permita.
- Bloquear a los usuarios el acceso a aplicaciones específicas o configurar una lista de aplicaciones permitidas y bloquear todas las demás.
- Vincular cuentas de VPP de Apple a UEM de modo que sea posible distribuir licencias adquiridas para las aplicaciones de asociadas a las cuentas de VPP.
- Configurar las aplicaciones de BlackBerry Dynamics públicas, ISV y personalizadas para permitir que los usuarios accedan a los recursos de trabajo.
- Conectar UEM a Microsoft Intune para que pueda establecer políticas de protección de la aplicación Intune desde dentro de la consola de administración de UEM para implementar y administrar aplicaciones de Office 365.
- Ver la lista de aplicaciones personales instaladas en los dispositivos.
- Permitir que los usuarios evalúen y revisen aplicaciones de otros usuarios de su entorno.
- Configurar los ajustes de notificación para las aplicaciones del sistema y las aplicaciones que gestiona mediante UEM.
- Especificar el icono y la etiqueta para icono de Work Apps en los dispositivos.

Comportamiento de la aplicación en los dispositivos con iOS con activaciones de Controles de MDM

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

Para dispositivos iOS activados con iPadOS y Controles de MDM, ocurre el comportamiento siguiente:

Tipo de aplicación	Cuando las aplicaciones están asignadas a un usuario	Cuando se actualizan las aplicaciones	Cuando las aplicaciones no están asignadas desde un usuario	Cuando se elimina el dispositivo de BlackBerry UEM
Aplicaciones públicas con una disposición obligatoria	En los dispositivos supervisados, las aplicaciones se instalan automáticamente. Si la aplicación ya está instalada, la gestiona UEM. En los dispositivos no supervisados, se pide a los usuarios que instalen las aplicaciones. Si ya se han instalado las aplicaciones, se le pregunta al usuario si desea permitirle a UEM gestionar las aplicaciones. Las aplicaciones se quitan de la lista "Nuevas/actualizaciones" cuando el usuario visualiza los detalles (incluso si la aplicación no está instalada), o cuando el usuario instala aplicaciones. Puede utilizar un perfil de cumplimiento para definir las acciones que se producen si no se instalan las aplicaciones obligatorias.	iTunes notifica a los usuarios de actualizaciones disponibles. Las aplicaciones se eliminarán de la lista "Nuevas/actualizaciones" cuando el usuario actualice la aplicación. (puede tardar hasta una hora) En los dispositivos que no tienen acceso a iTunes, los usuarios no reciben notificaciones, pero pueden descargar la actualización del catálogo de aplicaciones si al dispositivo se asigna una licencia VPP de Apple.	Las aplicaciones se eliminan automáticamente sin ninguna notificación. Las aplicaciones ya no aparecen en el catálogo de aplicaciones.	Las aplicaciones se eliminan automáticamente.

Tipo de aplicación	Cuando las aplicaciones están asignadas a un usuario	Cuando se actualizan las aplicaciones	Cuando las aplicaciones no están asignadas desde un usuario	Cuando se elimina el dispositivo de BlackBerry UEM
Aplicaciones públicas con una disposición opcional	Si las aplicaciones ya están instaladas en dispositivos supervisados, la aplicación se gestiona mediante UEM. En los dispositivos no supervisados, se solicita al usuario que permita que UEM gestione las aplicaciones. Se notifica al usuario cuando hay cambios en el catálogo de aplicaciones. Las aplicaciones se borran de la lista "nuevas/actualizadas" solo cuando el usuario visualiza los detalles (independientemente de si la aplicación está instalada). Los usuarios pueden elegir si desean instalar las aplicaciones.	iTunes notifica a los usuarios de actualizaciones disponibles. Las aplicaciones se borran de la lista "nuevas/actualizadas" cuando el usuario visualiza los detalles (independientemente de si la aplicación está actualizada).	Las aplicaciones se eliminan automáticamente sin ninguna notificación. Las aplicaciones ya no aparecen en el catálogo de aplicaciones.	Las aplicaciones se eliminan automáticamente.

Tipo de aplicación	Cuando las aplicaciones están asignadas a un usuario	Cuando se actualizan las aplicaciones	Cuando las aplicaciones no están asignadas desde un usuario	Cuando se elimina el dispositivo de BlackBerry UEM
Aplicaciones internas con una disposición obligatoria	En los dispositivos supervisados, las aplicaciones se instalan automáticamente. Si la aplicación ya está instalada, la gestiona UEM. En los dispositivos no supervisados, se pide a los usuarios que instalen las aplicaciones. Si ya se han instalado las aplicaciones, se le pregunta al usuario si desea permitirle a UEM gestionar las aplicaciones. Si el usuario cancela la instalación, puede instalar aplicaciones desde el catálogo de aplicaciones. Las aplicaciones se quitan de la lista "Nuevas/ actualizaciones" cuando el usuario visualiza los detalles (incluso si la aplicación no está instalada), o cuando el usuario instala aplicaciones. Puede utilizar un perfil de cumplimiento para definir las acciones que se producen si no se instalan las aplicaciones	Las aplicaciones se eliminarán de la lista "Nuevas/ actualizaciones" cuando el usuario actualice la aplicación.	Las aplicaciones se eliminan automáticamente sin ninguna notificación. Las aplicaciones ya no aparecen en el catálogo de aplicaciones.	Las aplicaciones se eliminan automáticamente.

Tipo de aplicación	Cuando las aplicaciones están asignadas a un usuario	Cuando se actualizan las aplicaciones	Cuando las aplicaciones no están asignadas desde un usuario	Cuando se elimina el dispositivo de BlackBerry UEM
Aplicaciones internas con una disposición opcional	Si las aplicaciones ya están instaladas en dispositivos supervisados, la aplicación se gestiona mediante UEM. En los dispositivos no supervisados, se solicita al usuario que permita que UEM gestione las aplicaciones. Las aplicaciones se quitan de la lista "Nuevas/ actualizaciones" cuando el usuario visualiza los detalles (incluso si la aplicación no está instalada), o cuando el usuario instala aplicaciones.	Las aplicaciones se eliminarán de la lista "Nuevas/ actualizaciones" cuando el usuario actualice la aplicación.	Las aplicaciones se eliminan automáticamente de los dispositivos activados con Controles de MDM sin enviar ninguna notificación. Las aplicaciones no se eliminan de los dispositivos activados con Privacidad del usuario. Las aplicaciones ya no aparecen en el catálogo de aplicaciones.	Las aplicaciones se eliminan automáticamente.

Para obtener información acerca del comportamiento de solicitud de instalación de aplicaciones, consulte Agregar una aplicación iOS a la lista de aplicaciones.

Comportamiento de la aplicación en los dispositivos con iOS con activaciones de Privacidad del usuario

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

Cuando activa dispositivos iOS y iPadOS con Privacidad del usuario, puede seleccionar si quiere permitir la administración de las aplicaciones. Si permite la administración de aplicaciones, el comportamiento de la aplicación con activaciones Privacidad del usuario será el mismo que con activaciones de Controles de MDM.

Si no permite la administración de aplicaciones en los dispositivos activados con Privacidad del usuario, el comportamiento será el siguiente:

Tipo de aplicación	Cuando las aplicaciones están asignadas a un usuario	Cuando se actualizan las aplicaciones	Cuando las aplicaciones no están asignadas desde un usuario	Cuando se elimina el dispositivo de BlackBerry UEM
Aplicaciones públicas con una disposición obligatoria	No se le solicitará al usuario que instale las aplicaciones. Los usuarios deben acceder al catálogo de aplicaciones para instalar las aplicaciones necesarias. Las aplicaciones se quitan de la lista "Nuevas/ actualizaciones" cuando el usuario visualiza los detalles (incluso si la aplicación no está instalada), o cuando el usuario instala aplicaciones.	iTunes notifica a los usuarios de actualizaciones disponibles. Las aplicaciones se eliminarán de la lista "Nuevas/ actualizaciones" cuando el usuario actualice la aplicación. (puede tardar hasta una hora) En los dispositivos que no tienen acceso a iTunes, los usuarios no reciben notificaciones, pero pueden descargar la actualización del catálogo de aplicaciones.	Las aplicaciones permanecen en el dispositivo. Las aplicaciones ya no aparecen en el catálogo de aplicaciones.	Las aplicaciones permanecen en el dispositivo.

Tipo de aplicación	Cuando las aplicaciones están asignadas a un usuario	Cuando se actualizan las aplicaciones	Cuando las aplicaciones no están asignadas desde un usuario	Cuando se elimina el dispositivo de BlackBerry UEM
Aplicaciones públicas con una disposición opcional	Si la aplicación ya está instalada, no ocurrirá nada. Se notifica al usuario cuando hay cambios en el catálogo de aplicaciones. Las aplicaciones se borran de la lista "nuevas/actualizadas" solo cuando el usuario visualiza los detalles (independientemente de si la aplicación está instalada). Los usuarios pueden elegir si desean instalar las aplicaciones.	iTunes notifica a los usuarios de actualizaciones disponibles. Las aplicaciones se borran de la lista "nuevas/actualizadas" cuando el usuario visualiza los detalles (independientemente de si la aplicación está actualizada).	Las aplicaciones permanecen en el dispositivo. Las aplicaciones ya no aparecen en el catálogo de aplicaciones.	Las aplicaciones permanecen en el dispositivo.
Aplicaciones internas con una disposición obligatoria	Si ya se han instalado las aplicaciones, se le pregunta al usuario si desea permitirle a UEM gestionar las aplicaciones. Las aplicaciones se quitan de la lista "Nuevas/actualizaciones" cuando el usuario visualiza los detalles (incluso si la aplicación no está instalada), o cuando el usuario instala aplicaciones.	Las aplicaciones se eliminarán de la lista "Nuevas/actualizaciones" cuando el usuario actualice la aplicación.	Las aplicaciones permanecen en el dispositivo. Las aplicaciones ya no aparecen en el catálogo de aplicaciones.	Las aplicaciones permanecen en el dispositivo.

Tipo de aplicación	Cuando las aplicaciones están asignadas a un usuario	Cuando se actualizan las aplicaciones	Cuando las aplicaciones no están asignadas desde un usuario	Cuando se elimina el dispositivo de BlackBerry UEM
Aplicaciones internas con una disposición opcional	Si las aplicaciones ya están instaladas, no ocurrirá nada. Las aplicaciones se quitan de la lista "Nuevas/ actualizaciones" cuando el usuario visualiza los detalles (incluso si la aplicación no está instalada), o cuando el usuario instala aplicaciones.	Las aplicaciones se eliminarán de la lista "Nuevas/ actualizaciones" cuando el usuario actualice la aplicación.	Las aplicaciones permanecen en el dispositivo. Las aplicaciones ya no aparecen en el catálogo de aplicaciones.	Las aplicaciones permanecen en el dispositivo.

Para obtener información acerca del comportamiento de solicitud de instalación de aplicaciones en un dispositivo, consulte Agregar una aplicación iOS a la lista de aplicaciones.

Activación de dispositivos con iOS

Cuando usted o un usuario activa un dispositivos con iOS o iPadOS con BlackBerry UEM, el dispositivo se asocia con BlackBerry UEM para que pueda administrar dispositivos y que los usuarios puedan acceder a los datos de trabajo desde sus dispositivos.

Puede activar dispositivos con BlackBerry UEM mediante el uso o sin él de Apple Configurator 2 para preparar los dispositivos para la activación. Para obtener más información acerca del uso de Apple Configurator 2, consulte Activación de dispositivos iOS con Apple Configurator 2 en el contenido referente a Administración

También puede inscribir los dispositivos en el programa de inscripción de dispositivos de Apple y asignar configuraciones de inscripción para dispositivos mediante la consola de gestión de BlackBerry UEM. Las configuraciones de inscripción incluyen reglas adicionales, tales como "Activar modo supervisado", que se asignan a los dispositivos durante la inscripción de MDM. Para obtener más información, consulte Activación de dispositivos con iOS que están inscritos en DEP en el contenido de Administración.

Si los dispositivos no se han inscrito en DEP, podrá seguir evitando que los dispositivos no supervisados se activen mediante el uso de la configuración del perfil de activación.

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 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	Puede utilizar el tipo de activación Privacidad del usuario para proporcionar un control básico de los dispositivos a la vez que se garantiza la privacidad de los datos personales de los usuarios. Con este tipo de activación, no se instala ningún contenedor independiente en el dispositivo y no se proporciona seguridad adicional para los datos de trabajo. Los dispositivos activados con Privacidad del usuario se activan en BlackBerry UEM y pueden utilizar servicios como Find my Phone y Root Detection, aunque 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 BlackBerry UEM puede acceder a la tarjeta SIM y a la información de hardware del dispositivo, como ICCID e IMEI, para comprobar si hay disponible una licencia SIM adecuada. • **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 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	Puede utilizar el tipo de activación Privacidad de usuario: inscripción de usuario para los dispositivos con iOS y iPadOS y así garantizar que los datos del usuario permanecen en privado 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 (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 con iPhone y iPad no supervisados con iOS y iPadOS 13.1 o posterior.
Registro del dispositivo solo para BlackBerry 2FA	Este tipo de activación es compatible con la solución de BlackBerry 2FA para dispositivos que BlackBerry UEM no administra. Este tipo de activación no proporciona ningún control o administración de dispositivos, pero permite que los dispositivos utilicen la característica BlackBerry 2FA. Para utilizar este tipo de activación, también debe asignar el perfil BlackBerry 2FA a los usuarios. Cuando se activa un dispositivo, puede ver información limitada de este en la consola de gestión y desactivar el dispositivo mediante un comando. Este tipo de activación solo es compatible con usuarios de Microsoft Active Directory. Los dispositivos Apple TV no admiten este tipo de activación. Para obtener más información, consulte el contenido de BlackBerry 2FA.

Creación de perfiles de activación

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

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

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

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

Creación de un perfil de activación

1. En la barra de menús, haga clic en **Políticas y perfiles**.

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

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

      Muchas versiones anteriores del SO ya no son compatibles con BlackBerry UEM. Solo debe seleccionar una versión mínima si no desea que sea compatible con la versión más antigua actualmente admitida por BlackBerry UEM. Para obtener más información sobre las versiones compatibles, consulte la Matriz de compatibilidad.
   d) Seleccione los tipos de activación compatibles.
10. 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. Para obtener más información acerca de cada opción, consulte Tipos de activación: Dispositivos iOS.
   c) Si ha seleccionado "Controles de MDM" o el tipo de activación "Privacidad del usuario" (con licencias basadas en SIM) y solo desea activar dispositivos supervisados, seleccione **No permitir activar dispositivos no supervisados**
   d) En la sección **Comprobar la integridad de la aplicación de iOS**, seleccione opcionalmente 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 están activados para comprobar 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 comprobar 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 BlackBerry UEM. Para obtener más información, consulte el contenido de BlackBerry Protect Mobile.

11. Haga clic en **Agregar**.

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

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

Estos pasos se aplican a dispositivos iOS y iPadOS que se activan mediante Controles de MDM o Privacidad del usuario con las opciones de MDM activadas.

Durante la activación, los usuarios deben salir de la aplicación BlackBerry UEM Client para instalar manualmente el perfil de MDM. El modo de bloqueo debe estar desactivado en el dispositivo (iOS y iPadOS 16 o posterior). El modo de bloqueo impide la instalación de los perfiles de configuración necesarios para la activación.

Envíe las siguientes instrucciones de activación al usuario del dispositivo o envíele un enlace al siguiente flujo de trabajo: Activación de su dispositivo iOS.

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. Instale BlackBerry UEM Client en el dispositivo. Puede descargar BlackBerry UEM Client en la App Store.
2. En el dispositivo, toque **UEM Client** y acepte el acuerdo de licencia.
3. 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 BlackBerry 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 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 mensaje de correo de activación que ha recibido o en BlackBerry UEM Self-Service. **c.** Toque **Siguiente**.

4. Toque **Permitir** para permitir que UEM Client envíe notificaciones. Si selecciona **No permitir**, impedirá que el dispositivo se active por completo.

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 **Gestión de perfiles y 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 BlackBerry UEM Client para completar la activación.
11. Si se le solicita, siga las instrucciones que aparecen en pantalla para instalar las aplicaciones de trabajo en su dispositivo.

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

- En el dispositivo, abra la aplicación BlackBerry UEM Client y toque **Acerca de**. En las secciones Dispositivo activado y Estado de conformidad, compruebe que aparezcan la información de dispositivo y la marca de tiempo de activación.
- 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 usuario de Apple es compatible con los dispositivos con iPad y iPadOS 13.1 o versiones posteriores.

Para iniciar la inscripción, el usuario debe utilizar la aplicación de la cámara para escanear un QR Code proporcionado en el correo electrónico de activación de la inscripción de usuario de Apple y así poder descargar e instalar manualmente el perfil de MDM en el dispositivo. Para activar el dispositivo, el usuario debe iniciar sesión en su cuenta de ID de Apple gestionada que coincide con la dirección de correo electrónico de la cuenta de usuario de BlackBerry UEM. Debe asignar UEM Client utilizando una licencia VPP a los usuarios si desea permitirles que puedan activar otras aplicaciones de BlackBerry Dynamics, importar certificados, utilizar características de BlackBerry 2FA, utilizar CylancePROTECT y comprobar el estado de conformidad. La configuración de UEM Client comienza cuando el usuario acepta el acuerdo de licencia.

Envíe las instrucciones de activación siguientes al usuario del dispositivo.

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 ID de Apple 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 ya ha caducado, puede solicitar un nuevo código de activación desde BlackBerry UEM Self-Service o ponerse en contacto con su administrador.

2. Abra la aplicación de la cámara de su dispositivo 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 la aplicación BlackBerry UEM Client, toque en **Instalar** cuando se le solicite, o abra Aplicaciones de trabajo.
11. Para configurar la aplicación BlackBerry UEM Client, ábrala 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 la aplicación BlackBerry UEM Client y toque **Acerca de**. En las secciones Dispositivo activado y Estado de conformidad, compruebe que aparezcan la información de dispositivo y la marca de tiempo de activación.
- 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.

Administración y control de dispositivos activados

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

Tiene las siguientes opciones:

Opción	Descripción
Compruebe si hay actualizaciones de software disponibles y actualice el dispositivo	Puede ver las actualizaciones del sistema operativo para todos los dispositivos administrados. Puede forzar los dispositivos supervisados para instalar una actualización. Para obtener más información, consulte el contenido de Administración.
Active la configuración de ubicación y el Modo perdido	Puede activar la configuración de ubicación para realizar un seguimiento de la ubicación de los dispositivos. También puede activar el Modo perdido para encontrar un dispositivo perdido. Para obtener más información, consulte el contenido de Administración.
Activar bloqueo de activación	La función de bloqueo de activación de los dispositivos requiere que los usuarios confirmen ID y la contraseña de Apple para desactivar Buscar mi iPhone, eliminar los datos del dispositivo o volver a activar y utilizar el dispositivo. Para gestionar la función de bloqueo de activación en BlackBerry UEM: • El dispositivo debe supervisarse. • El dispositivo debe tener configurada una cuenta de iCloud. • El dispositivo debe tener activada la opción Buscar mi iPhone o Buscar mi iPad. BlackBerry UEM almacena un código de desvío que puede utilizar para eliminar el bloqueo, de modo que los datos del dispositivo pueden borrarse y reactivarse sin el ID y la contraseña de Apple del usuario. Para obtener más información, consulte el contenido de Administración.
Recuperación de registros del dispositivo	Puede recuperar registros de dispositivos para fines de control y resolución de problemas. Para obtener más información, consulte el contenido de Administración.
Desactivar un dispositivo	Cuando usted o un usuario desactiva el dispositivo, la conexión entre el dispositivo y la cuenta de usuario en BlackBerry UEM se elimina. No se puede gestionar el dispositivo y ya no aparece en la consola de gestión. El usuario no puede acceder a los datos de trabajo en el dispositivo. Puede desactivar un dispositivo mediante los comandos "Eliminar todos los datos del dispositivo" o "Eliminar solo los datos de trabajo". Los usuarios pueden desactivar un dispositivo mediante la selección de la opción Desactivar mi dispositivo en la pantalla Acerca de la aplicación BlackBerry UEM Client.

Enviar un comando a un dispositivo

Antes de empezar:

Si desea establecer un periodo de caducidad para los comandos que eliminan datos de los dispositivos con BlackBerry UEM, consulte Establecer un tiempo de caducidad para los comandos.

1. En la barra de menús, haga clic en **Usuarios > Dispositivos gestionados**.
2. Busque una cuenta de usuario.
3. En los resultados de la búsqueda, haga clic en el nombre de la cuenta de usuario.
4. Haga clic en la pestaña del dispositivo.
5. En la ventana **Gestionar dispositivo**, seleccione el comando que desee enviar al dispositivo.

Comandos para dispositivos con iOS

Estos comandos también se aplican a los dispositivos con iPadOS.

Comando	Descripción	Tipos de activación
Ver informe del dispositivo	Este comando muestra información detallada acerca de un dispositivo. Puede exportar y guardar el informe del dispositivo en el equipo. Para obtener más información, consulte Ver y guardar un informe de dispositivo.	Controles de MDM Privacidad del usuario
Ver acciones de dispositivo	Este comando muestra todas las acciones que están en curso en un dispositivo. Para obtener más información, consulte Ver acciones de dispositivo.	Controles de MDM Privacidad del usuario
Eliminar todos los datos del dispositivo	Este comando elimina toda la información de usuario y los datos de aplicaciones que el dispositivo guarda y devuelve el dispositivo a la configuración predeterminada de fábrica. Si el dispositivo no se puede conectar a BlackBerry UEM cuando envía este comando, puede cancelar el comando o eliminar el dispositivo de la consola. Si el dispositivo se conecta a BlackBerry UEM una vez que lo elimine, solo se eliminarán los datos de trabajo del dispositivo. Para enviar este comando a varios dispositivos, consulte Envío de un comando masivo.	Controles de MDM

Comando	Descripción	Tipos de activación
Eliminar solo los datos de trabajo	Este comando elimina datos de trabajo, incluidas las políticas de TI, los perfiles, las aplicaciones y los certificados que se encuentran en un dispositivo. Si el dispositivo no se puede conectar a BlackBerry UEM cuando envía este comando, puede cancelar el comando o eliminar el dispositivo de la consola. Si el dispositivo se conecta a BlackBerry UEM una vez que lo elimine, se eliminarán los datos de trabajo del dispositivo. Para enviar este comando a varios dispositivos, consulte Envío de un comando masivo.	Controles de MDM Privacidad del usuario
Bloquear dispositivo	Este comando bloquea un dispositivo. El usuario debe escribir la contraseña del dispositivo para desbloquear el dispositivo. Si un dispositivo se pierde de manera temporal, puede utilizar este comando. Cuando se envía este comando, el dispositivo se bloquea solo si existe una contraseña para el dispositivo. De lo contrario, no se realiza ninguna acción en el dispositivo. Este comando no es compatible con dispositivos Apple TV.	Controles de MDM
Desbloquear y borrar contraseña	Este comando desbloquea un dispositivo y elimina la contraseña. Al usuario se le indica que cree una contraseña para el dispositivo. Puede utilizar este comando si el usuario olvida la contraseña del dispositivo. Este comando no es compatible con dispositivos Apple TV.	Controles de MDM
Activar modo perdido	Este comando bloquea el dispositivo y le permite establecer un número de teléfono y un mensaje que se mostrará en el dispositivo. Por ejemplo, puede mostrar la información de contacto cuando se encuentre el dispositivo. Después de enviar este comando, podrá ver la ubicación del dispositivo desde BlackBerry UEM. Este comando solo es compatible con dispositivos supervisados. Este comando no es compatible con dispositivos Apple TV.	Controles de MDM
Desactivar BlackBerry 2FA	Este comando desactiva los dispositivos que se activan con el tipo de activación "BlackBerry 2FA". El dispositivo se elimina de BlackBerry UEM y el usuario no puede utilizar la característica BlackBerry 2FA. Este comando no es compatible con dispositivos Apple TV.	Controles de MDM

Comando	Descripción	Tipos de activación
Actualizar SO	Este comando fuerza los dispositivos a instalar una actualización del SO. Para obtener más información, consulte Actualización del sistema operativo en dispositivos iOS supervisados. Para enviar este comando a varios dispositivos, consulte Envío de un comando masivo. Este comando solo es compatible con dispositivos supervisados. Este comando no es compatible con dispositivos Apple TV.	Controles de MDM
Reiniciar dispositivo	Este comando fuerza a los dispositivos a reiniciarse. Este comando solo es compatible con dispositivos supervisados. Este comando no es compatible con dispositivos Apple TV.	Controles de MDM
Desactivar dispositivo	Este comando fuerza a los dispositivos a desactivarse. Este comando solo es compatible con dispositivos supervisados. Este comando no es compatible con dispositivos Apple TV.	Controles de MDM
Limpiar aplicaciones	Este comando borra los datos de todas las aplicaciones gestionadas por Microsoft Intune en el dispositivo. Las aplicaciones no se eliminan del dispositivo. Para obtener más información, consulte Borrar aplicaciones gestionadas por Microsoft Intune.	Controles de MDM
Actualizar la información del dispositivo	Este comando envía y recibe información del dispositivo actualizada. Por ejemplo, puede enviar reglas de políticas de TI actualizadas recientemente o perfiles a un dispositivo y recibir información actualizada acerca de un dispositivo, como la versión del SO o el nivel de la batería. Para enviar este comando a varios dispositivos, consulte Envío de un comando masivo.	Controles de MDM Privacidad del usuario
Actualizar zona horaria	Este comando establece la hora del dispositivo en función de la región que seleccione.	Controles de MDM

Comando	Descripción	Tipos de activación
Eliminar dispositivo	Este comando elimina el dispositivo de BlackBerry UEM, pero no borra los datos del dispositivo. El dispositivo puede seguir recibiendo correos electrónicos y otros datos de trabajo. Este comando está destinado para los dispositivos que se hayan dañado o perdido de forma irreversible y no se espere que vuelvan a contactar con el servidor. Si un dispositivo que se haya eliminado intenta contactar con BlackBerry UEM, el usuario recibe una notificación y el dispositivo no podrá comunicarse con BlackBerry UEM a menos que se reactive. Para enviar este comando a varios dispositivos, consulte Envío de un comando masivo.	Controles de MDM Privacidad del usuario
Actualización de planes móviles eSIM	Para dispositivos que tienen un plan de telefonía móvil basado en eSIM, este comando consulta los detalles del plan actualizado para el dispositivo desde la URL del operador del dispositivo.	Controles de MDM

Aviso legal

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

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

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

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

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

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

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

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

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

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

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

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

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

Publicado en Canadá