BlackBerry UEM para sitios oscuros

Instalación y Administración

12.16

Contents

Acerca de BlackBerry UEM para sitios oscuros

BlackBerry UEM es una solución multiplataforma EMM de BlackBerry que ofrece una administración exhaustiva de dispositivos, aplicaciones y contenido con seguridad y conectividad integradas.

En entornos con los requisitos de seguridad más elevados, la conexión a sitios externos tales como BlackBerry Infrastructure puede estar restringida o ser imposible. BlackBerry UEM para sitios oscuros se ha diseñado para proporcionar una solución de gestión de dispositivos móviles segura sin necesidad de que BlackBerry UEM se conecte a BlackBerry Infrastructure y otros servicios por Internet.

Funciones de BlackBerry UEM compatibles

Las siguientes funciones de BlackBerry UEM son compatibles en un entorno de sitio oscuro.

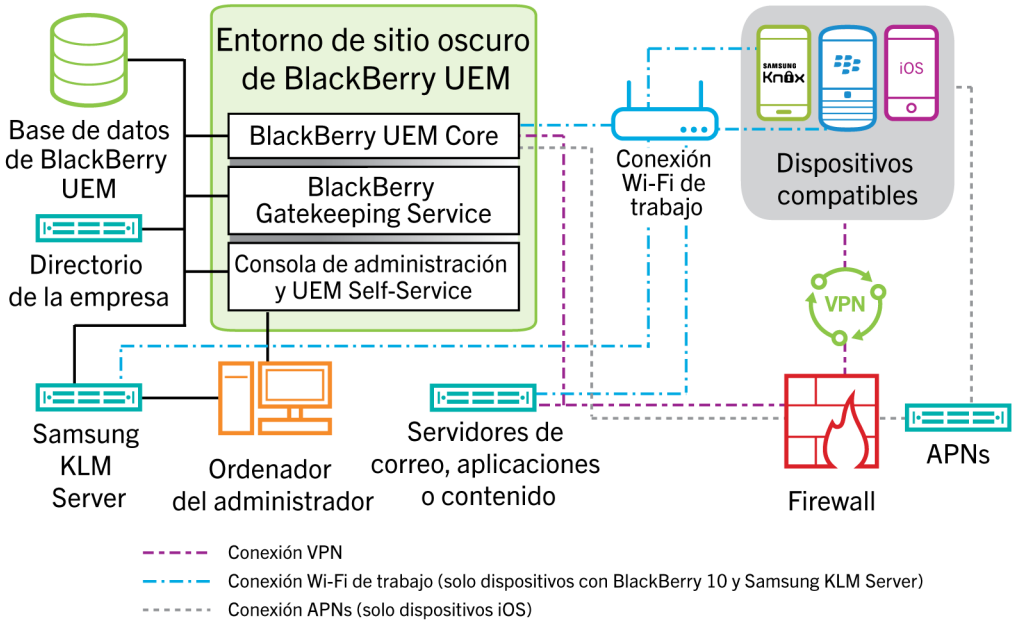
Función	Descripción
Administración de dispositivos multiplataforma	Puede administrar dispositivos con BlackBerry 10, iOS y Samsung Knox.
Experiencia segura y fiable	Los controles de dispositivos le ofrecen una administración precisa de la forma en que se conectan los dispositivos a su red, las capacidades activadas y las aplicaciones disponibles.
Control del acceso a Microsoft Exchange	Su empresa puede utilizar el BlackBerry Gatekeeping Service para controlar qué dispositivos pueden acceder a Exchange ActiveSync. Cualquier dispositivo que no esté en la lista blanca de Microsoft Exchange se notifica en la lista UEM de dispositivos restringidos de Exchange ActiveSync y se le bloquea el acceso al correo de trabajo y los datos del organizador.
Administración de aplicaciones	Puede instalar y administrar aplicaciones internas en dispositivos. También puede bloquear dispositivos para impedir la instalación de aplicaciones desde otras fuentes.
Administración basada en funciones	Puede compartir las labores administrativas con otros administradores que pueden acceder a las consolas de administración a la vez. Se pueden utilizar funciones para definir las acciones que puede realizar un administrador y reducir los riesgos de seguridad, distribuir las responsabilidades del trabajo y aumentar la eficacia con la limitación de las opciones disponibles para cada administrador. Puede utilizar las funciones predefinidas o bien crear sus propias funciones personalizadas.

Funciones de BlackBerry UEM no compatibles

Las siguientes funciones de BlackBerry UEM no son compatibles en un entorno de sitio oscuro. Estas funciones están desactivadas en BlackBerry UEM para sitios oscuros.

Funciones no compatibles	Explicación
Dispositivos	BlackBerry UEM para sitios oscuros solo admite dispositivos con BlackBerry 10, iOS y Samsung.
Conectividad de la empresa	Las funciones de BlackBerry UEM que permiten a los dispositivos conectarse a los recursos de su organización a través de BlackBerry Infrastructure no son compatibles, incluidas: • BlackBerry Secure Connect Plus • BlackBerry Secure Gateway • BlackBerry MDS Connection Service • Utilización de BlackBerry UEM como proxy para solicitudes SCEP
BlackBerry Dynamics	Las aplicaciones de BlackBerry Dynamics, incluida BlackBerry Work, no son compatibles.
Productos empresariales adicionales de BlackBerry	BlackBerry UEM para sitios oscuros no funciona con otros productos empresariales de BlackBerry, incluidos: • BlackBerry Enterprise Identity • BlackBerry 2FA
Gestión de aplicaciones públicas y aplicaciones protegidas por Microsoft Intune	BlackBerry UEM para sitios oscuros no es compatible con conexiones con proveedores de aplicaciones públicas como BlackBerry World, AppleApp Store y Google Play. No puede agregar aplicaciones públicas a los dispositivos de los usuarios. BlackBerry UEM para sitios oscuros no es compatible con conexiones a Microsoft Azure. No se pueden gestionar las aplicaciones mediante perfiles de protección de aplicaciones Microsoft Intune.

Arquitectura: BlackBerry UEM para sitios oscuros



Nombre del componente	Descripción
BlackBerry UEM Core	BlackBerry UEM Core es el componente central de la arquitectura de BlackBerry UEM. Está constituido por varios subcomponentes que se encargan de: • Registro, supervisión, presentación de informes y funciones de administración • Los servicios de autenticación y autorización • Programación y envío de comandos, políticas de TI y perfiles a los dispositivos
Base de datos de BlackBerry UEM	La base de datos de BlackBerry UEM es una base de datos relacional que contiene información de la cuenta de usuario y la información de configuración que BlackBerry UEM utiliza para administrar dispositivos.
BlackBerry Gatekeeping Service	BlackBerry Gatekeeping Service envía los comandos a Exchange ActiveSync para agregar dispositivos a una lista de dispositivos admitidos cuando los dispositivos están activados en BlackBerry UEM. Los dispositivos no administrados que intentan conectarse a un servidor de correo de la empresa pueden ser revisados, verificados, así como bloqueados o admitidos por un administrador a través de la consola de gestión de BlackBerry UEM.
Consola de gestión y UEM Self-Service	La consola de gestión y UEM Self-Service proporcionan una interfaz de usuario basada en navegador para que el usuario y el administrador accedan a BlackBerry UEM. Puede usar esta consola para gestionar la configuración del sistema, los usuarios, los dispositivos y las aplicaciones. Los usuarios pueden usar UEM Self-Service para establecer una contraseña de activación y enviar comandos a los dispositivos tales como configurar contraseña, bloquear el dispositivo y eliminar los datos de los dispositivos.

Nombre del componente	Descripción
Servidores de correo, aplicaciones o contenido	Su red interna incluye varios servicios con los que los dispositivos y BlackBerry UEM pueden comunicarse. Si está activando dispositivos Samsung Knox mediante tipos de activación Android Enterprise, necesita un servidor que contenga el archivo .apk de BlackBerry UEM Client y un archivo PAC que impida que los dispositivos intenten conectarse a Google Play durante la activación.
Servidor Samsung KLM	Si está administrando dispositivos Samsung Knox, se instala un servidor de administración de licencias de Samsung Knox con BlackBerry UEM para sitios oscuros, de modo que BlackBerry UEM no tenga que conectarse al sistema de administración de licencias de Samsung Knox basado en web para obtener la información de la licencia. Los dispositivos Samsung Knox se comunican con el servidor KLM mediante la red Wi-Fi de trabajo.
APN	Para administrar dispositivos con iOS, BlackBerry UEM debe enviar notificaciones a los dispositivos a través de un servidor de APN. Cuando los dispositivos reciben una notificación de APN, se ponen en contacto con BlackBerry UEM para buscar actualizaciones. Para obtener más información acerca de las conexiones seguras a APN o posibles alternativas al uso de APN públicas, póngase en contacto con su representante de soporte de Apple.

Instalación o actualización de BlackBerry UEM en un entorno de sitio oscuro

Solo los siguientes componentes están activados para BlackBerry UEM instalado en un entorno de sitio oscuro:

- Consola de gestión de BlackBerry UEM
- BlackBerry UEM Core
- BlackBerry Gatekeeping Service

Puede actualizar BlackBerry UEM. Para obtener información acerca de la migración de dispositivos a un nuevo entorno de BlackBerry UEM, consulte el contenido de Configuración de BlackBerry UEM.

Al instalar o actualizar BlackBerry UEM, puede utilizar un Microsoft SQL Server existente o instalar y utilizar Microsoft SQL Server Express.

Nota: Antes de instalar o actualizar BlackBerry UEM, revise los requisitos y requisitos previos en el contenido de Planificación de BlackBerry UEM y en el contenido de Instalación y actualización. Los requisitos de puerto se encuentran en el contenido de Planificación.

Instalación o actualización de BlackBerry UEM

1. Inicie sesión como usuario con privilegios de administrador local en el servidor en el que instala o actualiza BlackBerry UEM.
2. Descargue y extraiga los archivos de instalación de BlackBerry UEM.
3. Modifique el archivo deployer.properties con los parámetros de su entorno. El archivo deployer.properties está ubicado en la misma carpeta que el archivo setup.exe.
   a) En el campo **service.account.password=**, escriba la contraseña de la cuenta con la que se ha registrado.
   b) Si desea utilizar un Microsoft SQL Server existente, escriba la información en los campos correspondientes para ese servidor.

   Para obtener información acerca de cómo rellenar los campos, consulte el archivo deployer.properties en el contenido de Instalación y actualización de BlackBerry UEM.
4. Abra una ventana del símbolo del sistema como administrador y en el directorio del que se extrajeron los archivos de instalación de BlackBerry UEM, escriba uno de los siguientes comandos:

Opción	Comando
Para utilizar una base de datos de Microsoft SQL Server existente	`setup.exe --script --iacceptbeseula --propertyFiles darksite.properties --showlog`
Para instalar una base de datos local de Microsoft SQL Server	`setup.exe --script --iacceptbeseula --propertyFiles darksite.properties --showlog --installSQL`

Inicio de sesión en BlackBerry UEM

Después de instalar BlackBerry UEM, inicie sesión en la consola de administración.

Nota: Cuando inicie sesión en BlackBerry UEM por primera vez, además de proporcionar el nombre de su organización, el identificador de SRP y la clave de autenticación de SRP, debe introducir el **nombre de archivo de licencia**. Obtenga un archivo de licencia de su representante de ventas de BlackBerry. El identificador de SRP y la clave de autenticación de SRP deben coincidir con la información del archivo de licencia.

PRECAUCIÓN: No vuelva a utilizar el ID de SRP de instancias anteriores de BES5, BES10, BES12 o BlackBerry UEM al instalar una nueva instancia de BlackBerry UEM.

Inicio de sesión en BlackBerry UEM por primera vez

Antes de empezar: Verifique que el identificador de SRP y la clave de autenticación de SRP de BlackBerry UEM estén disponibles.

Si la aplicación de configuración está todavía abierta, puede acceder a la consola de gestión directamente desde el cuadro de diálogo Direcciones de consolas.

1. En el navegador, escriba **https://docs.blackberry.com/es/endpoint-management/blackberry-uem-cloud/latest/administration://<*nombre del servidor*>:<*puerto*>/admin**, donde <*nombre del servidor*> es el FQDN del equipo que aloja la consola de gestión. El puerto predeterminado para la consola de gestión es el puerto 443.
2. En el campo **Nombre de usuario**, escriba **admin**.
3. En el campo **Contraseña**, escriba **password**.
4. Haga clic en **Iniciar sesión.**
5. En la lista desplegable Ubicación del servidor, seleccione el país del equipo que tiene BlackBerry UEM instalado y haga clic en **Siguiente**.
6. Escriba el nombre de la empresa, el identificador de SRP y la clave de autenticación de SRP.
7. Haga clic en **Submit**.
8. Cambie la contraseña temporal a una contraseña permanente.
9. Haga clic en **Submit**.

Después de terminar:

- Cuando inicie sesión en la consola de gestión, puede elegir entre completar o cerrar el cuadro de diálogo **Le damos la bienvenida a BlackBerry UEM**. Si cierra el cuadro de diálogo, no aparece durante los posteriores inicios de sesión.

Configuración de BlackBerry UEM para sitios oscuros

La siguiente tabla resume las tareas de configuración que puede que necesite realizar después de instalar BlackBerry UEM en un entorno de sitio oscuro.

Para obtener más información sobre la configuración de BlackBerry UEM, consulte el contenido de Configuración de BlackBerry UEM.

Tarea	Descripción
Importar un archivo de licencia de BlackBerry UEM	Debe importar manualmente la información de licencia en BlackBerry UEM un entorno de sitio oscuro. Para obtener más información, consulte Adición de licencias a BlackBerry UEM.
Sustitución de los certificados predeterminados por certificados de confianza	Puede sustituir el certificado SSL predeterminado que utilizan las consolas de BlackBerry UEM y el certificado predeterminado que BlackBerry UEM utiliza para firmar el perfil de MDM para los dispositivos con iOS por certificados de confianza. Para obtener más información, consulte Cambiar certificados BlackBerry UEM en el contenido de Configuración de BlackBerry UEM.
Configuración de conexiones a través de servidores de proxy internos	Si su empresa utiliza un servidor proxy para las conexiones entre servidores dentro de la red, es posible que tenga que configurar los ajustes de proxy del lado del servidor para permitir a BlackBerry UEM Core comunicarse con las instancias remotas de la consola de gestión. Para obtener más información, consulte Configuración de conexiones a través de servidores de proxy internos en la configuración de contenido de BlackBerry UEM.
Conexión de BlackBerry UEM a los directorios de la empresa	Puede conectar BlackBerry UEM a uno o varios directorios de la empresa para que BlackBerry UEM pueda acceder a los datos del usuario para crear cuentas de usuario. Para obtener más información, consulte Conexión con los directorios de la empresa en la configuración de contenido de BlackBerry UEM.
Conexión de BlackBerry UEM a un servidor SMTP	Si desea que BlackBerry UEM envíe mensajes de correo de activación y otras notificaciones a los usuarios, debe especificar la configuración del servidor SMTP que BlackBerry UEM puede utilizar. Para obtener más información, consulte Conexión a un servidor SMTP para enviar notificaciones de correo en la configuración de contenido de BlackBerry UEM.
Adquisición y registro de un certificado APN	Si desea gestionar y enviar datos a los dispositivos con iOS, debe obtener una CSR firmada de BlackBerry, utilizarla para obtener un certificado APN de Apple y registrar el certificado APN con el dominio de BlackBerry UEM. Para obtener más información, consulte Adquisición de certificado APN para gestionar los dispositivos iOS.

Tarea	Descripción
Control de los dispositivos que pueden acceder a Exchange ActiveSync	Si se ha configurado Microsoft Exchange para impedir que los dispositivos accedan al correo de trabajo y a los datos del organizador a menos que se hayan agregado a una lista de permitidos, deberá crear una configuración de Microsoft Exchange en BlackBerry UEM. Para obtener más información, consulte Supervisión de los dispositivos que pueden acceder a Exchange ActiveSync en el contenido de administración de BlackBerry UEM.
Configuración de BlackBerry UEM Self-Service	Si desea permitir a los usuarios realizar determinadas tareas de gestión, como cambiar sus contraseñas, puede configurar y distribuir la aplicación web de BlackBerry UEM Self-Service. Para obtener más información, consulte Configuración de BlackBerry UEM Self-Service para los usuarios en el contenido de administración de BlackBerry UEM.

Adición de licencias a BlackBerry UEM

Al instalar BlackBerry UEM en un entorno de sitio oscuro, debe importar manualmente información de la licencia a BlackBerry UEM.

Si está administrando dispositivos de Samsung Knox, también debe establecer claves de licencia de Samsung Knox y claves de licencia KLM.

Para evitar actualizar manualmente las licencias en el futuro, especialmente para dispositivos Samsung Knox, considere la posibilidad de comprar licencias perpetuas para el entorno de sitio oscuro de su organización.

Puede obtener un archivo de licencia de BlackBerry UEM y las claves de licencia de Samsung de su representante de ventas de BlackBerry.

Importación de licencias de BlackBerry UEM

Antes de empezar: Obtenga un archivo de licencia de BlackBerry UEM de su representante de ventas de BlackBerry.

1. En la barra de menús, haga clic en **Configuración > Licencias**.
2. En la página **Resumen de licencias**, haga clic en **Importar licencia**.
   Si desea actualizar las licencias existentes, en su lugar, haga clic en **Actualizar licencias**.
3. Haga clic en **Examinar**.
4. Seleccione el archivo de licencia que desea utilizar.
5. Haga clic en **Abrir**.

Configuración de claves de licencia de Samsung Knox

Si está administrando dispositivos Samsung Knox en un entorno de sitio oscuro, debe establecer claves de licencia de Samsung Knox en BlackBerry UEM.

Antes de empezar: Obtenga claves de licencia de Samsung Knox y claves de licencia KLM de su representante de ventas de BlackBerry.

1. En la barra de menús, haga clic en **Configuración > Licencias**.

2. En la página **Resumen de licencias**, haga clic en **Establecer claves de licencia de KNOX**.
3. Pegue la clave de licencia de Samsung Knox ELM y la clave de licencia de Samsung Knox KLM en los campos correspondientes.
4. Haga clic en **Guardar**.

Adquisición de certificado APN para gestionar los dispositivos iOS

APN es el servicio de Apple Push Notification. Para administrar dispositivos iOS, Apple requiere que BlackBerry UEM pueda conectarse a la APN. Para obtener más información acerca de las conexiones seguras a APN o posibles alternativas al uso de APN públicas, póngase en contacto con su representante de soporte de Apple.

Debe obtener y registrar un certificado APN para utilizar BlackBerry UEM para gestionar dispositivos iOS.

Nota: El certificado APN es válido durante un año. La consola de gestión muestra la fecha de caducidad. Deberá renovar el certificado APN antes de la fecha de caducidad, a través del mismo ID de Apple que utilizó para obtener el certificado. Si el certificado caduca, los dispositivos no reciben datos de BlackBerry UEM. Si desea registrar un nuevo certificado APN, los usuarios deberán reactivar los dispositivos para recibir datos.

Para obtener más información, visite https://developer.apple.com y lea *Problemas con el envío de notificaciones de inserción* en el artículo TN2265.

Se recomienda acceder a la consola de gestión y al portal de certificados de inserción de Apple mediante los navegadores Google Chrome o Safari. Estos navegadores proporcionan una compatibilidad óptima para solicitar y registrar un certificado APN.

Para obtener y registrar un certificado APN para utilizar APN públicas, lleve a cabo las siguientes acciones:

Paso	Acción
1	Obtención de una CSR firmada de BlackBerry.
2	Usar la CSR firmada para solicitar un certificado APN de Apple.
3	Registro del certificado APN.

Obtención de una CSR firmada de BlackBerry

Deberá obtener una CSR firmada de BlackBerry antes de que pueda obtener un certificado APN.

1. En la barra de menú, haga clic en **Configuración > Integración externa > Apple Push Notification**.
2. Haga clic en **Obtener certificado APN**.

   Si desea renovar el certificado APN actual, haga clic en **Renovar certificado** en su lugar.
3. En la sección **Paso 1 de 3: Descargar el certificado CSR firmado de BlackBerry**, haga clic en **Descargar solicitud de firma del certificado**.
4. Haga clic en **Guardar** para guardar el archivo CSR sin firmar (.scsr) en el equipo.
5. Envíe el archivo CSR sin firmar a su representante de atención al cliente de BlackBerry.

   Su representante de atención al cliente hará que el archivo CSR se firme mediante una CA de BlackBerry y le enviará el CSR firmado.

Después de terminar: Solicitar un certificado APN de Apple.

Solicitar un certificado APN de Apple

Antes de empezar: Obtención de una CSR firmada de BlackBerry.

1. En la barra de menú, haga clic en **Configuración > Integración externa > Apple Push Notification**.
2. En la sección **Paso 2 de 3: Solicitar un certificado APN de Apple**, haga clic en **Portal de certificados de inserción de Apple**. Se le dirige al portal de certificados de inserción de Apple.
3. Inicie sesión en el portal de certificados de inserción de Apple a través de un ID de Apple válido.
4. Siga las instrucciones para cargar la CSR firmada (.scsr).
5. Descargue y guarde el certificado APN (.pem) en el equipo.

Después de terminar: Registro del certificado APN.

Registro del certificado APN

Antes de empezar: Solicitar un certificado APN de Apple.

1. En la barra de menú, haga clic en **Configuración > Integración externa > Apple Push Notification**.
2. En la sección **Paso 3 de 3: Registrar el certificado APN**, haga clic en **Examinar**. Vaya al certificado APN (.pem) y selecciónelo.
3. Haga clic en **Submit**.

Después de terminar: Para probar la conexión entre BlackBerry UEM y el servidor de APN, haga clic en **Probar certificado APN**.

Administración de usuarios y dispositivos en un entorno de sitio oscuro

Las tareas de administración de usuarios y dispositivos para la mayoría de las funciones compatibles en un entorno de sitio oscuro son las mismas que en cualquier otro entorno de BlackBerry UEM. Para obtener instrucciones sobre la mayoría de las tareas administrativas no cubiertas en este documento, consulte el contenido de Administración de BlackBerry UEM.

Activación del dispositivo

Cuando active un dispositivo, podrá asociarlo a BlackBerry UEM de modo que pueda administrar el dispositivo y que los usuarios puedan acceder a los datos de trabajo en el dispositivo.

Al activar un dispositivo, puede enviar las políticas de TI y los perfiles para controlar las características disponibles 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.

Tipos de activación compatibles

BlackBerry UEM para sitios oscuros es compatible con los siguientes tipos de activación de dispositivos con BlackBerry 10, Samsung Knox y iOS.

Dispositivos BlackBerry 10

Tipo de activación	Descripción
Trabajo y personal - Empresa	Este tipo de activación proporciona el control de los datos del trabajo en los dispositivos, al tiempo que garantiza la máxima privacidad de los datos personales. Al activar un dispositivo, 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 del trabajo se protegen mediante cifrado y autenticación por contraseña. Todos los datos de trabajo de cualquiera de las activaciones previas se eliminan. Puede controlar el espacio de trabajo en el dispositivo mediante comandos y políticas de TI, pero no puede controlar ningún aspecto del espacio personal en el dispositivo.
Solo espacio de trabajo	Este tipo de activación proporciona un control total del dispositivo y no ofrece un espacio independiente para los datos personales. Al activar un dispositivo, el espacio personal y todos los datos de trabajo de cualquier activación previa se eliminan, se instala un espacio de trabajo y el usuario debe crear una contraseña para acceder al dispositivo. Los datos del trabajo se protegen mediante cifrado y autenticación por contraseña. Puede controlar el dispositivo a través de comandos y políticas de TI.

Tipo de activación	Descripción
Trabajo y personal - Regulado	Este tipo de activación proporciona control tanto sobre los datos personales como sobre los del trabajo. Al activar un dispositivo, 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 del trabajo se protegen mediante cifrado y autenticación por contraseña. Todos los datos de trabajo de cualquiera de las activaciones previas se eliminan. Puede controlar tanto el espacio de trabajo como el espacio personal en el dispositivo a través de comandos y políticas de TI.

Dispositivos Samsung Knox

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

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

Tipo de activación	Descripción
Trabajo y personal: control total (dispositivo Android Enterprise completamente gestionado con perfil de trabajo)	Este tipo de activación le permite administrar todo el dispositivo con comandos y reglas de políticas de TI. Este tipo de activación crea un perfil de trabajo en el dispositivo que separa los datos de trabajo y los datos personales. Los datos en el espacio de trabajo estarán protegidos mediante cifrado y un método de autenticación como una contraseña, un PIN, un patrón o una huella digital. Este tipo de activación es compatible con el registro de actividad del dispositivo (SMS, MMS y llamadas telefónicas) en archivos de registro de BlackBerry UEM. Tras la activación, los dispositivos con el tipo de activación Trabajo y personal: control total solo tienen un conjunto limitado de aplicaciones estándar preinstaladas, como Cámara, Teléfono y Ajustes, en el espacio personal. Este tipo de activación requiere que el dispositivo se restablezca a la configuración predeterminada de fábrica antes de la activación. Si se elimina BlackBerry UEM Client o se borra el perfil de trabajo del dispositivo, este se restablece automáticamente en los valores predeterminados de fábrica. Durante la activación los usuarios deberán conceder los permisos de administrador a BlackBerry UEM Client.
Trabajo y personal: privacidad de usuario (Android Enterprise con perfil de trabajo)	Este tipo de activación conserva la privacidad de los datos personales, pero le permite administrar los datos de trabajo con comandos y reglas de políticas de TI. Este tipo de activación crea un perfil de trabajo en el dispositivo que separa los datos de trabajo y los datos personales. Los datos personales y los datos de trabajo están protegidos mediante el cifrado y la autenticación de contraseña. Los usuarios no tienen que conceder permisos de administrador a BlackBerry UEM Client.
Solo espacio de trabajo - (Samsung Knox)	Este tipo de activación le permite administrar todo el dispositivo con comandos y reglas de políticas de TI de Samsung Knox. Este tipo de activación elimina el espacio personal e instala un espacio de trabajo. El usuario debe crear una contraseña para acceder al dispositivo. Todos los datos del dispositivo estarán protegidos mediante cifrado y un método de autenticación, como una contraseña, un PIN, un patrón o una huella digital. Este tipo de activación es compatible con el registro de actividad del dispositivo (SMS, MMS y llamadas telefónicas) en archivos de registro de BlackBerry UEM. Durante la activación los usuarios deberán conceder los permisos de administrador a BlackBerry UEM Client.
Trabajo y personal: control total (Samsung Knox)	Este tipo de activación le permite administrar todo el dispositivo con comandos y reglas de políticas de TI de Samsung Knox. Este tipo de activación crea un espacio de trabajo independiente en el dispositivo y el usuario debe crear una contraseña para acceder al espacio de trabajo. Los datos en el espacio de trabajo estarán protegidos mediante cifrado y un método de autenticación como una contraseña, un PIN, un patrón o una huella digital. Este tipo de activación es compatible con el registro de actividad del dispositivo (SMS, MMS y llamadas telefónicas) en archivos de registro de BlackBerry UEM. Durante la activación los usuarios deberán conceder los permisos de administrador a BlackBerry UEM Client.

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. En el dispositivo no hay instalado un espacio de trabajo independiente y no existe seguridad adicional para los datos de trabajo. Puede controlar el dispositivo a través de comandos y políticas de TI.

Preparación de los usuarios para activar dispositivos

Para prepararse para permitir a los usuarios activar dispositivos, deberá crear un perfil de activación, modificar la plantilla de correo de activación y establecer una contraseña de activación para el usuario.

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 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 coincidan 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. El perfil de activación predeterminado permite opciones de activación que no son compatibles en un entorno de sitio oscuro. 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.

La plantilla de correo de activación define el mensaje de correo enviado a los usuarios indicándoles que activen su dispositivo.

Cuando se ha completado el perfil y la plantilla de correo de activación, puede establecer una contraseña de activación para el usuario y enviar un mensaje de correo de activación para permitirle completar la activación.

Creación de un perfil de activación

Nota: El perfil de activación muestra las opciones de tipo de dispositivo y activación que no son compatibles en un entorno de sitio oscuro. Al crear o actualizar un perfil de activación, no seleccione opciones no compatibles.

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 **Propietario del dispositivo**, lleve a cabo una de las siguientes acciones:
   - Seleccione **No especificado** si algunos usuarios activan dispositivos personales y algunos usuarios activan los dispositivos de trabajo.
   - Seleccione **Trabajo** si la mayoría de los usuarios activan dispositivos de trabajo.
   - Seleccione **Personal** si la mayoría de los usuarios activan sus 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 BlackBerry 10 o iOS 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 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 solo a algunos modelos.
      - **No permitir modelos de dispositivo seleccionados**: Los usuarios no podrán activar los modelos de dispositivo que especifique. 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 permitida del SO.

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

      Para los dispositivos con Samsung Knox, puede seleccionar varios tipos de activación y clasificarlos. Para todos los demás tipos de dispositivos, puede seleccionar solo un tipo de activación.
10. Para los dispositivos con iOS, si solo desea activar dispositivos supervisados, seleccione **No permitir activar dispositivos no supervisados**
11. Para los dispositivos con Samsung, realice las siguientes acciones:
   a) Si ha seleccionado más de un tipo de activación, haga clic en las flechas hacia arriba y abajo para clasificarlos.
   b) Si ha seleccionado un tipo de activación Android Enterprise, seleccione **Al activar dispositivos con Android Enterprise, active las funciones premium de UEM como BlackBerry Secure Connect Plus**, para activar las funciones de Knox Platform for Enterprise.
   c) Anule la selección de **Agregar cuenta de Google Play al espacio de trabajo**.

      La función no es compatible en un entorno de sitio oscuro.
   d) En la sección **Opciones de atestación de hardware**, seleccione **Aplicar reglas de cumplimiento de atestación durante la activación** si desea que BlackBerry UEM envíe comprobaciones a los dispositivos cuando se activan para garantizar que está instalado el nivel de revisión de seguridad necesario.
12. Haga clic en **Agregar**.

Creación de una plantilla de correo de activación

1. En la barra de menú, haga clic en **Configuración** > **Configuración general**.
2. Haga clic en **Plantillas de correo electrónico**.
3. Haga clic en +. Seleccione **Activación de dispositivos**.
4. En el campo **Nombre**, escriba un nombre para identificar la plantilla.
5. En el campo **Asunto**, edite el texto para personalizar la línea de asunto del primer correo de activación.
6. En el campo **Mensaje**, escriba el texto del cuerpo del correo electrónico de activación.

- Utilice el editor HTML para seleccionar el formato de fuente y para insertar imágenes (por ejemplo, un logotipo de empresa).
- Inserte variables en el texto para personalizar el mensaje (por ejemplo, puede utilizar la variable %UserDisplayName% para insertar el nombre del destinatario). Para obtener una lista de variables, consulte el contenido de Administración de BlackBerry UEM.
- Para dispositivos con BlackBerry 10 y Samsung Knox, incluya la dirección del servidor de BlackBerry UEM que los usuarios necesitan para activar el dispositivo.
  - Para dispositivos con BlackBerry 10, la URL es: http://*nombre.servidor*:8882/*ID_SRP*/mdm
  - Para dispositivos con Samsung Knox, la URL es: http://*nombre.servidor*:8882/*ID_SRP*
- Para ver texto de ejemplo, haga clic en **Texto sugerido**.

7. Para enviar la contraseña de activación separada de otras instrucciones de activación, seleccione **Enviar dos correos electrónicos de activación individuales: uno para las instrucciones completas y otro para la contraseña**. Si decide enviar solo un correo de activación, asegúrese de incluir la contraseña de activación o la variable de la contraseña de activación en el primer correo.
8. En el campo **Asunto**, escriba una línea de asunto para el segundo correo de activación.
9. Personalice el texto del cuerpo del segundo correo de activación que envía a los usuarios. Asegúrese de que se incluyen la contraseña de activación o la variable de la contraseña de activación.
10. 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 de activación a un usuario con la información necesaria para activar uno o más dispositivos.

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, 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. En el panel de Detalles de activación, haga clic en **Establecer contraseña de activación**.
5. En la lista desplegable **Opción de activación**, seleccione **Activación del dispositivo predeterminada**.
6. En la lista desplegable **Contraseña de activación**, realice una de las tareas 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**.
7. De manera opcional, puede cambiar la caducidad del periodo de activación. La caducidad del periodo de activación especifica cuánto tiempo la contraseña de activación sigue siendo válida.
8. 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**.
9. En la lista desplegable **Plantilla del correo de activación**, seleccione la plantilla de correo que desea usar.
10. Haga clic en **Submit**.

Activación de dispositivos BlackBerry 10

Puede permitir a los usuarios activar dispositivos con BlackBerry 10 a través de su red de trabajo Wi-Fi, o puede activar varios dispositivos con BlackBerry 10 para los usuarios con BlackBerry Wired Activation Tool.

Activación de dispositivos con BlackBerry 10 a través de una Wi-Fi de trabajo

Puede permitir a los usuarios que activen dispositivos con BlackBerry 10 a través de su red Wi-Fi de trabajo. Para activar dispositivos, los usuarios necesitan la siguiente información:

- Dirección de correo de trabajo
- Contraseña de activación
- Dirección del servidor de BlackBerry UEM (http://*nombre.servidor*:8882/*ID_SRP*/mdm)

Puede proporcionar la información en el correo de activación que BlackBerry UEM envía a los usuarios. Consulte Creación de una plantilla de correo de activación.

Activar un dispositivo BlackBerry 10

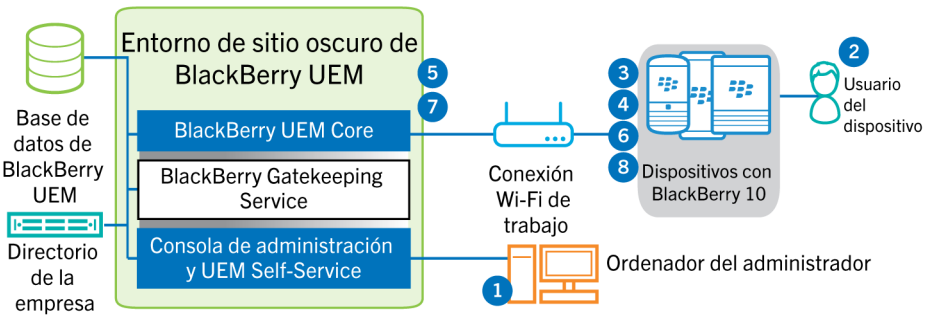
Envíe las instrucciones de activación siguientes al usuario del dispositivo.

1. En el dispositivo, diríjase a **Configuración**.
2. Toque **Cuentas**.
3. Si tiene cuentas en este dispositivo, toque **Agregar cuenta**. De lo contrario, continúe con el paso 4.
4. Toque **Correo, calendario y contactos**.
5. Escriba su dirección de correo de trabajo y toque **Siguiente**.
6. En el campo **Contraseña**, escriba la contraseña de activación que recibió. Toque **Siguiente**.
   Recibirá un aviso de que el dispositivo no ha podido buscar la información de conexión.
7. Toque **Avanzado**.
8. Toque **Cuenta de trabajo**.
9. En el campo **Dirección del servidor**, 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.
10. Toque **Hecho**.
11. 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, diríjase al BlackBerry Hub y confirme que aparece la dirección de correo. Vaya al calendario y confirme que aparecen las citas.
- 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.

Flujo de datos: activación de un dispositivo BlackBerry 10



1. Lleve a cabo las acciones siguientes:
   a. Agregue un usuario a BlackBerry UEM como una cuenta de usuario local o mediante la información de la cuenta recuperada desde el directorio de la empresa.
   b. Asigne un perfil de activación al usuario
   c. Utilice una de las siguientes opciones para proporcionar al usuario los detalles de activación:
      - Genere automáticamente una contraseña de activación del dispositivo y envíe un mensaje de correo electrónico con las instrucciones de activación al usuario
      - Establezca una contraseña de activación del dispositivo y comunique el nombre de usuario y la contraseña al usuario directamente o por correo electrónico
      - Anule la configuración de la contraseña de activación y comunique la dirección de BlackBerry UEM Self-Service al usuario para que pueda establecer su propia contraseña de activación
2. El usuario realiza las siguientes acciones:
   a. Se conecta a la red del trabajo Wi-Fi
   b. Escribe el nombre de usuario y la contraseña de activación en el dispositivo
   c. Para una activación "Trabajo y personal - Regulado" o "Solo espacio de trabajo", acepta el aviso de la empresa, que describe los términos y condiciones con los que el usuario debe estar de acuerdo
3. Si se trata de una activación "Solo espacio de trabajo", el dispositivo elimina todos los datos existentes y se reinicia.
4. El dispositivo realiza las siguientes acciones:
   a. Establece una conexión con BlackBerry UEM
   b. Genera una clave simétrica compartida que se utiliza para proteger la CSR y la respuesta a BlackBerry UEM mediante la contraseña de activación y EC-SPEKE.
   c. Crea unas CRS y HMAC cifradas de la siguiente manera:
      - Genera un par de claves para el certificado
      - Crea un PKCS#10 CSR que incluye la clave pública del par de claves
      - Cifra la CSR mediante la clave simétrica compartida y el AES-256 en modo CBC con el relleno PKCS#5
      - Calcula una HMAC de la CSR cifrada mediante SHA-256 y la adjunta a la CSR
   d. Envía la CSR y la HMAC cifradas a BlackBerry UEM
5. BlackBerry UEM realiza las siguientes acciones:
   a. Comprueba la HMAC de la CSR cifrada y descifra la CSR mediante la clave simétrica compartida
   b. Recupera el nombre de usuario, el ID del espacio de trabajo y el nombre de la empresa desde la base de datos de BlackBerry UEM
   c. Empaqueta un certificado de cliente con la información que ha recuperado y la CSR que el dispositivo ha enviado
   d. Firma el certificado de cliente mediante el certificado raíz de administración de la empresa
   e. Cifra el certificado de cliente, el certificado raíz de administración de la empresa y la URL de BlackBerry UEM mediante la clave simétrica compartida y el AES-256 en el modo CBC con el relleno PKCS#5
   f. Calcula la HMAC del certificado de cliente cifrado, el certificado raíz de administración de la empresa y la URL de BlackBerry UEM y lo adjunta a los datos cifrados
   g. Envía los datos cifrados y la HMAC al dispositivo
6. El dispositivo realiza las siguientes acciones:
   a. Verifica la HMAC
   b. Descifra los datos que ha recibido de BlackBerry UEM
   c. Almacena el certificado de cliente y el certificado raíz de administración de la empresa en su almacén de claves

7. BlackBerry UEM realiza las siguientes acciones:
   a. Asigna el nuevo dispositivo a una instancia de BlackBerry UEM en el dominio
   b. Envía la información de configuración, incluyendo los ajustes de conectividad de empresa al dispositivo
8. El dispositivo envía una confirmación a través de TLS a BlackBerry UEM para confirmar que ha recibido y aplicado la política de TI y otros datos, y que ha creado el espacio de trabajo. El proceso de activación se ha completado.

Los protocolos de curva elíptica utilizados durante el proceso de activación usan la curva de 521 bits recomendada por NITS.

Activación de dispositivos BlackBerry 10 mediante BlackBerry Wired Activation Tool

BlackBerry Wired Activation Tool permite activar varios dispositivos con BlackBerry 10 al mismo tiempo en entornos locales a través de conexiones USB en lugar de conexiones inalámbricas. Puede que la empresa desee usar este método por diferentes razones:

- Para hacer más rápida y fácil la activación de varios dispositivos a la vez
- Para mantener el proceso de activación en manos de los administradores
- Para activar los dispositivos y configurar las características de seguridad, tales como los requisitos de cifrado de contenido y perfiles VPN, antes de dárselos a los usuarios o conectarlos a la red de la empresa

No se pueden asignar perfiles y políticas mediante BlackBerry Wired Activation Tool. Debe asignar los perfiles y las políticas a los usuarios en la consola de gestión de BlackBerry UEM antes de asignar y activar dispositivos mediante BlackBerry Wired Activation Tool. Sin embargo, no es necesario establecer contraseñas de activación para asignar y activar dispositivos mediante BlackBerry Wired Activation Tool.

Para activar dispositivos mediante BlackBerry Wired Activation Tool, los dispositivos deben estar ejecutando BlackBerry 10 OS versión 10.3 o una versión posterior.

BlackBerry Wired Activation Tool no es compatible con BlackBerry UEM Cloud.

Para obtener BlackBerry Wired Activation Tool, póngase en contacto con el representante del servicio de asistencia técnica al cliente.

Configuración de BlackBerry Wired Activation Tool e inicio de sesión en una instancia de BlackBerry UEM

Antes de poder activar dispositivos con BlackBerry Wired Activation Tool, debe crear una configuración para cada instancia de BlackBerry UEM a la que necesite tener acceso. Después de crear una configuración, también debe utilizar una cuenta de administrador para permitir a BlackBerry Wired Activation Tool el acceso a BlackBerry Web Services.

1. En la carpeta de instalación de BlackBerry Wired Activation Tool, haga doble clic en el archivo **BWAT.exe**.
2. En **Agregar una pantalla de servidor de BES12**, en el campo **Nombre**, escriba un nombre para identificar la configuración que se va a crear. Por ejemplo, si tiene dos instancias de BlackBerry UEM, puede crear una configuración para cada una y darles un nombre, como Servidor 1 y Servidor 2.
3. En el campo **URL de BlackBerry Web Services**, escriba la dirección para el componente de BlackBerry Web Services. La dirección predeterminada es https://docs.blackberry.com/es/endpoint-management/blackberry-uem-cloud/latest/administration://*<dirección web de BlackBerry UEM>*:18084.

   El puerto se puede cambiar modificando el ajuste `tomcat.bws.port` en la base de datos de BlackBerry UEM.
4. En el campo **URL de extremo BCP**, escriba la dirección que se debe utilizar para las activaciones de dispositivos. Esto también se conoce como URL de activación o Nombre del servidor. La dirección predeterminada es: http://*nombre.servidor*:8882/*ID_SRP*/mdm.

Se puede encontrar la dirección asegurándose de que la variable %ActivationURL% está en la Plantilla del correo de activación y haciendo clic en **Ver correo electrónico de activación** desde cualquier pantalla de resumen de usuario.

Si es necesario, también puede buscar la dirección del host y el puerto en la base de datos de BlackBerry UEM. En la tabla `def_cfg_setting_dfn`, busque los valores `id_setting_definition` de `bdmi.enroll.bcp.host` y `bdmi.enroll.bcp.port`. A continuación, utilice los valores `id_setting_definition` para buscar los valores de los ajustes en `obj_global_cfg_Setting`.

5. Haga clic en **Submit**.
6. En la pantalla **Iniciar sesión**, seleccione una configuración de BlackBerry UEM de la lista desplegable.
7. En el campo **Nombre de usuario**, escriba el nombre de usuario de una cuenta de usuario de BlackBerry UEM con permisos de administrador.
8. En el campo **Contraseña**, escriba la contraseña de la cuenta.
9. En la lista desplegable **Directorio**, seleccione un método de autenticación.
10. Si es necesario, en el campo **Dominio**, escriba el dominio de Microsoft Active Directory.
11. Haga clic en **Conectar**.

Active los dispositivos BlackBerry 10 mediante BlackBerry Wired Activation Tool

Antes de empezar:

- Configuración de BlackBerry Wired Activation Tool e inicio de sesión en una instancia de BlackBerry UEM
- Encienda todos los dispositivos conectados y asegúrese de que, o todos los dispositivos han terminado el proceso de configuración inicial, o no lo han iniciado. No puede activar los dispositivos si el proceso de configuración inicial está en curso.

1. Conecte uno o más dispositivos BlackBerry 10 al equipo mediante cables USB.
2. Verifique la columna de **Estado** para cada dispositivo. Lleve a cabo una de las siguientes acciones:
   - Si en la columna Estado aparece **Requiere contraseña**, haga clic en **Requiere contraseña** para introducir la contraseña para el dispositivo
   - Si en la columna Estado aparece **Dispositivo no compatible**, actualice el software del dispositivo a BlackBerry 10 OS versión 10.3 o una versión posterior
   - Si en la columna Estado aparece **Preparado**, asigne el dispositivo a un usuario
3. En el campo **Buscar**, busque una cuenta de usuario a la que desea asignar un dispositivo.
4. En la lista de resultados de la búsqueda, haga clic en la cuenta de usuario.
5. En la sección principal de la pantalla, haga clic en un nombre de cuenta de usuario y arrastre el nombre hacia un dispositivo para asignar el dispositivo a dicho usuario. Repita el paso para asignar los dispositivos a varios usuarios.
6. Seleccione la casilla de verificación situada junto a los pares de usuarios y dispositivos que desea activar.
7. Haga clic en **Activar dispositivos**.

BlackBerry Wired Activation Tool activa todos los dispositivos seleccionados. Consulte la columna Estado para ver el progreso y los resultados de cada dispositivo. Si la activación no se completa, haga clic en el mensaje que aparece en la columna Estado para obtener más información acerca de los errores.

Activación de dispositivos con Samsung Knox

Los usuarios pueden activar dispositivos Samsung Knox a través de su red de trabajo Wi-Fi. BlackBerry UEM para sitios oscuros no es compatible con activaciones "Samsung Knox MDM" o "Trabajo y personal: privacidad

de usuario - (Samsung Knox)". BlackBerry UEM para sitios oscuros tampoco es compatible con Samsung Knox Mobile Enrollment.

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

Para activar dispositivos, los usuarios necesitan la siguiente información:

- Dirección de correo de trabajo
- Contraseña de activación
- Dirección del servidor de BlackBerry UEM (http://*nombre.servidor*:8882/*ID_SRP*)

Puede proporcionar la información en el correo de activación que BlackBerry UEM envía a los usuarios. Consulte Creación de una plantilla de correo de activación.

Si su organización está utilizando dispositivos Samsung Knox en un entorno de sitio oscuro, un servidor Samsung KLM se instala con BlackBerry UEM. Los dispositivos Samsung Knox se comunican con el servidor KLM mediante la red Wi-Fi de trabajo. Si está activando dispositivos con tipos de activación Android Enterprise y el certificado del servidor KLM está firmado por una CA interna, deberá enviar el certificado del servidor KLM a los dispositivos mediante un perfil de certificado de CA. Para obtener más información, consulte el contenido de administración de BlackBerry UEM.

Pasos para activar dispositivos Samsung Knox

Paso	Acción
1	Cree y asigne los perfiles, aplicaciones y políticas de TI necesarios a los usuarios. Si desea configurar una VPN para dispositivos Samsung Knox, Configuración de VPN mediante Knox StrongSwan.
2	Cree un perfil de activación y asígnelo a una cuenta de usuario o a un grupo de usuarios..
3	Establezca una contraseña de activación y envíe un mensaje de correo de activación.
4	Proporcione instrucciones de activación a los usuarios para dispositivos de Android Enterprise o dispositivos de Samsung Knox Workspace.

Instalación de BlackBerry UEM Client en dispositivos Samsung Knox

Los usuarios deben instalar BlackBerry UEM Client para activar un dispositivo Samsung Knox. Puede descargar UEM Client manualmente desde BlackBerry y guardarlo en una ubicación de red a la que los dispositivos tengan acceso. Para descargar el archivo .apk de la versión más reciente de UEM Client, visite support.blackberry.com/community y lea el artículo 42607.

Si los usuarios están activando dispositivos mediante los tipos de activación Samsung Knox Workspace o Android Enterprise (Trabajo y personal: privacidad de usuario), puede indicar a los usuarios que obtengan e instalen UEM Client antes de iniciar el proceso de activación.

Para los dispositivos que se vayan a activar con los tipos de activación Android Enterprise (Solo espacio de trabajo) o (Trabajo y personal: control total) deben restablecerse los valores predeterminados de fábrica del

dispositivo antes de comenzar la activación. Puede configurar las opciones de activación para instalar UEM Client desde un servidor de la red durante la activación. Para proporcionar la ubicación de descarga al dispositivo, puede incluir la ubicación en un QR Code que el usuario escanea para iniciar la activación.

Configuración de las opciones de activación para activaciones Android Enterprise

Para los dispositivos que se vayan a activar con los tipos de activación Android Enterprise (Solo espacio de trabajo) o (Trabajo y personal: control total) deben restablecerse los valores predeterminados de fábrica del dispositivo antes de comenzar la activación. Puede configurar las opciones de activación para instalar BlackBerry UEM Client desde un servidor de la red durante la activación. Para proporcionar la ubicación de descarga al dispositivo, puede incluir la ubicación en un QR Code que el usuario escanea para iniciar la activación.

También debe crear un archivo PAC que evite que los dispositivos intenten conectarse a Google Play durante la activación y almacenar el archivo PAC en la misma ubicación que el archivo .apk de UEM Client.

Antes de empezar: Descargue UEM Client desde BlackBerry y guárdelo en una ubicación de red a la que los dispositivos tengan acceso. Para obtener más información, visite support.blackberry.com/community para leer el artículo 42607.

1. Cree un archivo PAC con el siguiente formato que especifique la dirección URL HTTP en la que se aloja el archivo PAC y guárdelo en la misma ubicación que el archivo .apk de UEM Client.

   ```
   function FindProxyForURL(url, host)
   {
   return "DIRECT";
   }
   ```

   Los usuarios deberán especificar la **Dirección web de PAC** cuando configuren la conexión Wi-Fi en su dispositivo durante la activación. El archivo PAC debe estar disponible en el puerto HTTP 80 predeterminado.
2. En la barra de menús, haga clic en **Configuración > Configuración general**.
3. Haga clic en **Valores predeterminados de activación**.
4. En **Valores predeterminados de la activación del dispositivo**, ajuste las siguientes opciones de QR Code.
   a) Seleccione **Permitir códigos QR para la activación de dispositivos**.
   b) Seleccione **Permitir que el código QR contenga la ubicación del archivo de origen de la aplicación UEM Client**.
   c) En el campo **Ubicación del archivo de origen de la aplicación de UEM Client**, especifique la ubicación de red en la que guardó el archivo .apk.
5. Compruebe que no se han seleccionado las siguientes opciones:
   - **Activar el tipo de activación Controles MDM para dispositivos Android**
   - **Utilizar códigos QR para desbloquear aplicaciones de BlackBerry Dynamics**
   - **Activar registro con BlackBerry Infrastructure**
6. Haga clic en **Guardar**.

Activar un dispositivo Android Enterprise

Estas instrucciones se aplican a los tipos de activación Android Enterprise (Solo espacio de trabajo) o (Trabajo y personal: control total). Para estos dispositivos, el dispositivo debe establecerse en la configuración predeterminada de fábrica antes de iniciar la activación.

Para las activaciones de Android Enterprise (Trabajo y personal: privacidad de usuario), siga las instrucciones para Activar un dispositivo Samsung Knox Workspace.

Envíe las instrucciones de activación siguientes al usuario del dispositivo.

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

   Se abrirá un lector de códigos QR en el dispositivo.
3. Escanee el código QR proporcionado por su administrador.
4. Especifique la información para conectarse a la red Wi-Fi del trabajo, incluida la **Dirección web de PAC** proporcionada por el administrador.

   El dispositivo instala BlackBerry UEM Client y comienza el proceso de activación. El proceso de activación tarda varios minutos.
5. Responda a las solicitudes del dispositivo, incluida la introducción de la contraseña de activación si se solicita, la aceptación de cualquier acuerdo de licencia, la configuración de un perfil de trabajo y la creación de una contraseña de dispositivo.
6. Si es necesario, en función de la configuración del servidor, cuando se detenga la activación, conecte el dispositivo a un ordenador de la red mediante un cable USB-C antes de continuar.

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. Toque **Acerca de**. En la sección **Dispositivo activado**, 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.

Activar un dispositivo Samsung Knox Workspace

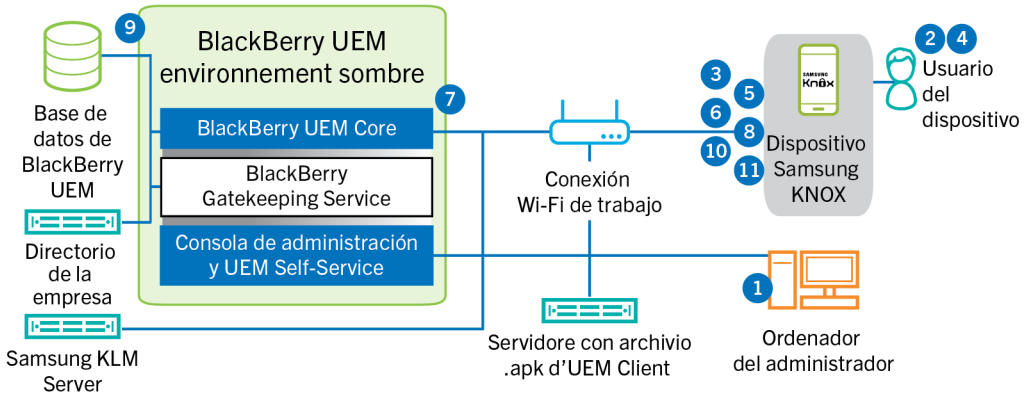
Estas instrucciones también se aplican a las activaciones de Android Enterprise (Trabajo y personal: privacidad de usuario). Envíe las instrucciones de activación siguientes al usuario del dispositivo.

1. Conecte el dispositivo a la red de trabajo Wi-Fi.
2. Descargue e instale BlackBerry UEM Client desde la ubicación proporcionada por el administrador.
3. En el dispositivo, toque **UEM Client**.
4. Lea el contrato de licencia. Toque **Acepto**.
5. Escriba su dirección de correo electrónico de trabajo. Toque **Siguiente**.
6. Escriba la dirección del servidor. Toque **Siguiente**. Puede encontrar la dirección del servidor en el mensaje de correo de activación que ha recibido o en BlackBerry UEM Self-Service.
7. Escriba una contraseña de activación. Toque **Activar mi dispositivo**.
8. Toque **Siguiente**.
9. Toque **Activar**.

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. Toque **Acerca de**. En la sección **Dispositivo activado**, 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.

Flujo de datos: activación de un dispositivo Android Enterprise

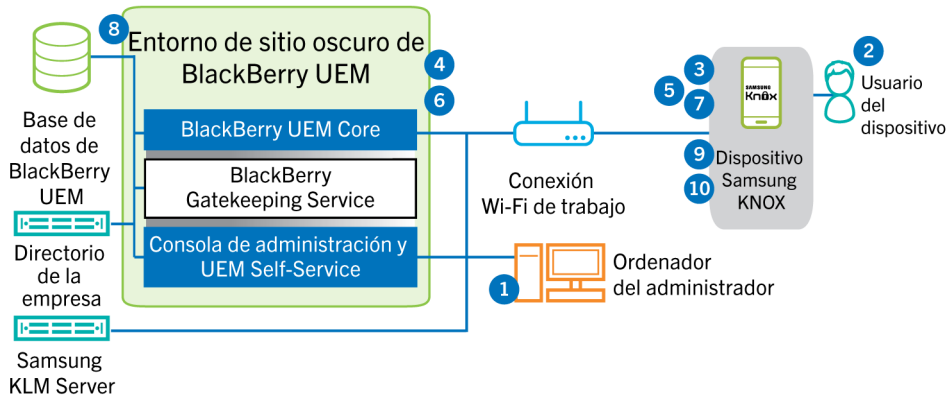


Este flujo de datos se aplica a los dispositivos activados con los tipos de activación Android Enterprise (Solo espacio de trabajo) o (Trabajo y personal: control total).

1. Lleve a cabo las acciones siguientes:
   a. Agregue un usuario a BlackBerry UEM como una cuenta de usuario local o mediante la información de la cuenta recuperada desde el directorio de la empresa
   b. Asegúrese de que se ha asignado al usuario el tipo de activación "Android Enterprise (Solo espacio de trabajo)" o "Trabajo y personal: control total"
   c. Configure los códigos QR de activación para que incluyan la contraseña de activación y la ubicación desde la que debe descargarse BlackBerry UEM Client.
2. El usuario restablece la configuración predeterminada de fábrica del dispositivo.
3. El dispositivo se reinicia y muestra una pantalla de bienvenida o de inicio.
4. El usuario realiza las siguientes acciones:
   a. Abre el correo electrónico de activación que ha recibido en su ordenador o en otro dispositivo
   b. Toca la pantalla del dispositivo siete veces para abrir un lector de códigos QR
   c. Conecte el dispositivo a la red de trabajo Wi-Fi
   d. Escanea el código QR del correo electrónico de activación
5. El dispositivo realiza las siguientes acciones:
   a. Solicita al usuario que cifre el dispositivo y lo reinicie
   b. Descarga UEM Client de la ubicación de descarga especificada por el código QR y lo instala
6. UEM Client establece una conexión con BlackBerry UEM y envía una solicitud de activación a BlackBerry UEM. La solicitud de activación incluye el nombre de usuario, la contraseña, el sistema operativo del dispositivo y el identificador único del dispositivo.
7. BlackBerry UEM lleva a cabo las siguientes acciones:
   a. Inspecciona la validez de las credenciales
   b. Crea una instancia del dispositivo
   c. Asocia la instancia del dispositivo a la cuenta de usuario especificada en la base de datos de BlackBerry UEM
   d. Agrega el ID de la sesión de inscripción a una sesión HTTP
   e. Envía un mensaje de autenticación satisfactoria al dispositivo
8. UEM Client solicita toda la información de configuración y envía la información del dispositivo y del software a BlackBerry UEM.
9. BlackBerry UEM almacena la información del dispositivo y envía la información de configuración al dispositivo.

10. UEM Client determina si el dispositivo utiliza Knox Platform for Enterprise y si ejecuta una versión compatible. Si el dispositivo utiliza Knox Platform for Enterprise, el dispositivo se conecta al servidor de Samsung KLM local y activa la licencia de administración de Knox. Tras la activación, UEM Client aplica las reglas de la política de TI de Android Enterprise.
11. El dispositivo envía una confirmación a BlackBerry UEM de que la ha recibido y aplica la información de configuración. El proceso de activación se ha completado.

Flujo de datos: Activación de un dispositivo para usar Knox Workspace



1. Lleve a cabo las acciones siguientes:
   a. Agregue un usuario a BlackBerry UEM como una cuenta de usuario local o mediante la información de la cuenta recuperada desde el directorio de la empresa.
   b. Asegúrese de haber asignado al usuario el tipo de activación "Trabajo y personal: control total (Samsung Knox)" o "Solo espacio de trabajo - (Samsung Knox)".
   c. Indique al usuario que descargue e instale BlackBerry UEM Client:
   d. Utilice una de las siguientes opciones para proporcionar al usuario los detalles de activación:
      - Genere automáticamente una contraseña de activación del dispositivo y envíe un mensaje de correo electrónico con las instrucciones de activación al usuario
      - Establezca una contraseña de activación del dispositivo y comunique el nombre de usuario y la contraseña al usuario directamente o por correo electrónico
      - Anule la configuración de la contraseña de activación y comunique la dirección de BlackBerry UEM Self-Service al usuario para que pueda establecer su propia contraseña de activación
2. El usuario realiza las siguientes acciones:
   - Se conecta a la red del trabajo Wi-Fi
   - Descarga e instala UEM Client en el dispositivo
   - Abre UEM Client e introduce la dirección de correo y la contraseña de activación
3. UEM Client establece una conexión con BlackBerry UEM y envía una solicitud de activación a BlackBerry UEM. La solicitud de activación incluye el nombre de usuario, la contraseña, el sistema operativo del dispositivo y el identificador único del dispositivo.
4. BlackBerry UEM lleva a cabo las siguientes acciones:
   a. Inspecciona la validez de las credenciales
   b. Crea una instancia del dispositivo
   c. Asocia la instancia del dispositivo a la cuenta de usuario especificada en la base de datos de BlackBerry UEM
   d. Agrega el ID de la sesión de inscripción a una sesión HTTP
   e. Envía un mensaje de autenticación satisfactoria al dispositivo

5. UEM Client crea una CSR con la información recibida de BlackBerry UEM y envía una solicitud de certificado de cliente a BlackBerry UEM a través de HTTPS.
6. BlackBerry UEM realiza las siguientes acciones:
   a. Valida la solicitud del certificado de cliente con el ID de la sesión de inscripción en la sesión HTTP
   b. Firma la solicitud del certificado de cliente con el certificado raíz
   c. Envía el certificado de cliente firmado y el certificado raíz de nuevo a UEM Client

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

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

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

Activación de dispositivos iOS

Si permite a los usuarios utilizar dispositivos iOS en un entorno de sitio oscuro, debe preparar los dispositivos utilizando Apple Configurator 2. BlackBerry UEM no es compatible con dispositivos inscritos en el programa de inscripción de dispositivos de Apple. Los usuarios completan la activación de los dispositivos preparados sin utilizar la aplicación BlackBerry UEM Client. Solo se requiere su nombre de usuario y la contraseña de activación.

Cuando los dispositivos están activados, BlackBerry UEM envía los perfiles y la política de TI que ha asignado a los usuarios en los dispositivos.

Pasos para activar dispositivos iOS

Paso	Acción
1	Adición de información del servidor de BlackBerry UEM a Apple Configurator 2.
2	Preparación de dispositivos iOS con Apple Configurator 2.
3	Cree un perfil de activación y asígnelo a una cuenta de usuario o a un grupo de usuarios..
4	Establezca una contraseña de activación y envíe un mensaje de correo de activación.

Paso	Acción
5	Distribuya los dispositivos a los usuarios y solicite que completen la instalación.

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 BlackBerry UEM con el formato: *<http o https>://<nombreservidor>:<puerto>*, donde el número de puerto predeterminado es 8885. Para obtener más información acerca de la configuración de los puertos, consulte Puertos de escucha de BlackBerry UEM en el contenido de Instalación y actualización.
5. Haga clic en **Siguiente**.
6. Cierre la ventana **Servidor**.

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 que puedan completar la activación.

Gestionar dispositivos con BlackBerry 10

Para obtener más información acerca de la administración de dispositivos y usuarios de dispositivos con BlackBerry 10, consulte el contenido de Administración de BlackBerry UEM.

Debe tener en cuenta las siguientes consideraciones a la hora de administrar dispositivos BlackBerry 10 en un entorno de sitio oscuro.

Consideraciones acerca del sitio oscuro	Descripción
Conectarse a los recursos de la empresa	En un entorno de sitio oscuro, los dispositivos con BlackBerry 10 pueden conectarse a su red utilizando solo su red de trabajo Wi-Fi o una VPN. Para utilizar una VPN, asegúrese de instalar una aplicación de VPN adecuada en el dispositivo y de configurar un perfil VPN.
Administración de aplicaciones	BlackBerry UEM para sitios oscuros no es compatible con conexiones a BlackBerry World. No puede agregar aplicaciones públicas a la lista de aplicaciones para dispositivos.

Gestionar dispositivos con Samsung Knox

Para obtener más información acerca de la administración de dispositivos y usuarios de dispositivos Samsung Knox, consulte el contenido de Administración de BlackBerry UEM.

Debe tener en cuenta las siguientes consideraciones a la hora de administrar dispositivos Samsung Knox en un entorno de sitio oscuro.

Consideraciones acerca del sitio oscuro	Descripción
Conectarse a los recursos de la empresa	En un entorno de sitio oscuro, después de la activación, los dispositivos Samsung Knox se pueden conectar a BlackBerry UEM y a sus recursos utilizando solo una conexión VPN. Para obtener más información, consulte "Configuración de VPN mediante Knox StrongSwan".
Administración de aplicaciones	BlackBerry UEM para sitios oscuros no es compatible con conexiones a Google Play. No puede agregar aplicaciones públicas a la lista de aplicaciones para dispositivos.
Correo y datos del organizador	La aplicación de correo predeterminada en dispositivos Samsung Knox necesita conectarse a la infraestructura Samsung antes de que pueda enviar y recibir datos. Puede elegir permitir esta conexión o utilizar otra aplicación de correo en los dispositivos Samsung Knox.
Notificaciones del dispositivo	Enviar notificaciones a dispositivos Samsung Knox mediante GCM no es compatible en un entorno de sitio oscuro. BlackBerry UEM Client buscará actualizaciones en BlackBerry UEM en intervalos regulares.

Configuración de VPN mediante Knox StrongSwan

Puede configurar el acceso VPN a su entorno para los dispositivos Samsung Knox.

Antes de empezar: Descargue las aplicaciones Knox Service Plugin y Android VPN Management for Knox StrongSwan y agregue los archivos .apk a la ubicación de red compartida para las aplicaciones internas.

1. Agregue las aplicaciones Knox Service Plugin y Android VPN Management for Knox StrongSwan a la lista de aplicaciones.

2. Seleccione la aplicación Knox Service Plugin y haga clic en + para ajustar las opciones de configuración de la aplicación.
   a) En **Perfil VPN**, seleccione **VPN propia de Knox**.
   b) En **Parámetros para la VPN propia de Knox para StrongSwan**, ajuste las siguientes opciones:
      - Ajuste el **Tipo de autenticación** a "ipsec_ike2_rsa".
      - Ajuste el **Alias del certificado de usuario** al nombre de usuario con "_1 [Knox]" agregado. Puede utilizar variables para el nombre de usuario (por ejemplo, `%UserFirstName% %UserLastName% _1 [Knox]`).
      - Ajuste el **Alias del certificado de CA** al nombre de usuario con " [Knox]" agregado. Puede utilizar variables para el nombre de usuario (por ejemplo, `%UserFirstName% %UserLastName% [Knox]`).
3. Asigne la aplicación al usuario.
4. Cree un perfil de certificado de CA para enviar el certificado del servidor VPN a los dispositivos y asignarlo a los usuarios.
5. Agregue un certificado de cliente de VPN para cada usuario.

Gestionar dispositivos con iOS

Para obtener más información acerca de la administración de dispositivos y usuarios de dispositivos iOS, consulte el contenido de Administración de BlackBerry UEM.

Debe tener en cuenta las siguientes consideraciones a la hora de administrar dispositivos iOS en un entorno de sitio oscuro.

Consideraciones acerca del sitio oscuro	Descripción
Conectarse a los recursos de la empresa	En un entorno de sitio oscuro, después de la activación, los dispositivos iOS se pueden conectar a BlackBerry UEM y sus recursos mediante una conexión VPN. Para utilizar una VPN, asegúrese de instalar una aplicación de VPN adecuada en el dispositivo y de configurar un perfil VPN.
Administración de aplicaciones	BlackBerry UEM para sitios oscuros no es compatible con conexiones a Apple App Store. No puede agregar aplicaciones públicas a la lista de aplicaciones para dispositivos.
Perfiles de conformidad	Dado que el cliente de BlackBerry UEM Client no es compatible con dispositivos iOS en un entorno de sitio oscuro, los perfiles de conformidad no son compatibles.

Documentación del producto

El siguiente contenido acerca de BlackBerry UEM debe ser útil a la hora de administrar BlackBerry UEM en un entorno de sitio oscuro.

Si sus requisitos de seguridad de sitio oscuro le impiden acceder a la documentación de BlackBerry UEM desde la consola de administración, puede descargar las versiones en PDF de la documentación desde una ubicación con acceso total a Internet o solicitar que su representante de atención al cliente de BlackBerry se las envíe.

Recurso	Descripción
Notas de la versión	• Descripciones de problemas solucionados • Descripción de problemas conocidos y posibles soluciones • Novedades
Instalación y actualización	• Requisitos del sistema • Instrucciones de instalación • Instrucciones de actualización
Configuración	• Instrucciones para saber cómo configurar los componentes del servidor antes de comenzar a administrar los usuarios y sus dispositivos • Instrucciones para migrar datos desde una base de datos de BlackBerry UEM existente
Administración	• Administración básica y avanzada para todos los tipos de dispositivos compatibles • Instrucciones para la creación de cuentas de usuario, grupos, funciones y cuentas de administrador • Instrucciones para la activación de dispositivos • Instrucciones para la creación y asignación de políticas de TI y perfiles • Instrucciones para la administración de aplicaciones en los dispositivos • Descripciones de las opciones de perfiles • Descripciones de reglas de políticas de TI de dispositivos con BlackBerry 10, iOS y Android
Matriz de compatibilidad	• Lista de los sistemas operativos, los servidores de bases de datos y los navegadores compatibles con el servidor de BlackBerry UEM • Lista de sistemas operativos de dispositivos compatibles

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