BlackBerry UEM

Asegurar conexiones usando PKI

Administración

12.17

Contents

Certificados y PKI

Un certificado de PKI es un documento digital emitido por una CA que verifica la identidad del sujeto del certificado y vincula la identidad a una clave pública. Cada certificado tiene una clave privada correspondiente que se almacena por separado. La clave pública y la privada forman un par de claves asimétricas que se pueden utilizar para el cifrado de datos y la autenticación de identidad. Una autoridad de certificación (CA) firma el certificado para verificar que las entidades que confían en la autoridad de certificación también puedan confiar en el certificado.

En función de la capacidad del dispositivo y del tipo de activación, los dispositivos y las aplicaciones pueden utilizar los certificados para:

- Autenticar mediante SSL/TLS al conectarse a páginas web que utilizan HTTPS
- Autenticar con un servidor de correo del trabajo
- Autenticar con una red Wi-Fi de trabajo o de VPN
- Cifrar y firmar mensajes de correo mediante protección S/MIME

Varios de los certificados utilizados con distintos fines se pueden guardar en un dispositivo.

Pasos que deberá seguir para la utilización de los certificados

Al utilizar certificados de PKI con dispositivos o aplicaciones, realice las siguientes acciones:

Paso	Acción
1	Si es necesario, conecte BlackBerry UEM al software de PKI de su empresa.
2	Cree uno o más perfiles de certificados de CA para enviarlos a los dispositivos y las aplicaciones.
3	Cree perfiles SCEP, perfiles de credenciales de usuario o perfiles de certificado compartido, o cargue certificados para un usuario específico para enviar certificados de cliente a los dispositivos y las aplicaciones.
4	Si es necesario, asocie perfiles de certificado con perfiles de Wi-Fi, VPN o correo electrónico.
5	Si es necesario, asigne los perfiles de certificado a las cuentas de usuario, a los grupos de usuarios o a los grupos de dispositivos.
6	Si utiliza certificados con una aplicación de BlackBerry Dynamics, en la configuración de la aplicación seleccione "Permitir que las aplicaciones de BlackBerry Dynamics utilicen certificados de usuario, perfiles SCEP y perfiles de credenciales de usuario".

Integración de BlackBerry UEM con el software PKI de la empresa

Si su empresa utiliza una solución de PKI para proporcionar certificados, puede extender la autenticación basada en certificados proporcionada por los servicios de PKI a los dispositivos que gestiona con BlackBerry UEM.

Los productos de Entrust (por ejemplo, Entrust IdentityGuard y Entrust Authority Administration Services) y productos de OpenTrust (por ejemplo, OpenTrust PKI y OpenTrust CMS) proporcionan las CA que emiten certificados de cliente. Puede configurar una conexión con el software PKI de la empresa y utilizar los perfiles para enviar el certificado de CA y los certificados de cliente a los dispositivos.

Para los dispositivos con BlackBerry Dynamics, también puede configurar un conector de PKI que crea una conexión entre BlackBerry UEM y un servidor CA para inscribir certificados para las aplicaciones de BlackBerry Dynamics o utilizar una aplicación compatible con inscripción de certificados basada en aplicación como Purebred.

Conectar BlackBerry UEM al software de Entrust de la empresa

Para permitir BlackBerry UEM o enviar certificados emitidos por el software de Entrust de su organización (por ejemplo, Entrust IdentityGuard o Entrust Authority Administration Services) a los dispositivos y aplicaciones de BlackBerry Dynamics, podrá agregar una conexión al software de Entrust de su empresa para BlackBerry UEM.

Antes de empezar: Póngase en contacto con el administrador de Entrust de la empresa para obtener:

- la URL del servicio web MDM de Entrust
- la información de inicio de sesión de una cuenta de administrador de Entrust que pueda usar para conectar BlackBerry UEM al software de Entrust
- el certificado de CA de Entrust que contiene la clave pública (.der, .pem, o .cert); BlackBerry UEM utiliza este certificado para establecer conexiones SSL con el servidor de Entrust

1. En la barra de menús, haga clic en **Configuración**.
2. Haga clic en **Integración externa > Autoridad de certificación**.
3. Haga clic en **Agregar una conexión Entrust**.
4. En el campo **Nombre de la conexión**, escriba un nombre para la conexión.
5. En el campo **URL**, escriba la URL del servicio web MDM de Entrust.
6. En el campo **Nombre de usuario**, escriba el nombre de usuario de la cuenta del administrador de Entrust.
7. En el campo **Contraseña**, escriba la contraseña de la cuenta del administrador de Entrust.
8. Para cargar un certificado de CA con el fin de permitir que BlackBerry UEM establezca conexiones SSL con el servidor de Entrust, haga clic en **Examinar**. Navegue y seleccione el certificado de CA.
9. Para probar la conexión, haga clic en **Probar conexión**.
10. Haga clic en **Guardar**.

Después de terminar:

- Cree un perfil de credenciales de usuario para enviar certificados de su software de PKI a los dispositivos.

Conectar BlackBerry UEM al servidor de Entrust IdentityGuard de su empresa para utilizar credenciales inteligentes

Si su empresa utiliza credenciales inteligentes derivadas gestionadas por Entrust IdentityGuard, puede utilizar credenciales inteligentes derivadas con dispositivos Android y con aplicaciones de BlackBerry Dynamics en dispositivos iOS y Android.

Antes de empezar:

Póngase en contacto con el administrador de Entrust de la empresa para obtener la información siguiente:

- URL del servidor de Entrust IdentityGuard
- Nombre de la credencial inteligente que se va a activar en los dispositivos como se especifica en Entrust IdentityGuard
- Certificado de CA de Entrust para enviar el certificado a los dispositivos

1. En la barra de menús, haga clic en **Configuración**.
2. Haga clic en **Integración externa > Autoridad de certificación**.
3. Haga clic en **Añadir una conexión para credenciales inteligentes de Entrust**.
4. En el campo **Nombre de la credencial inteligente**, escriba el nombre de la credencial inteligente que se especifica en Entrust IdentityGuard.
5. En el campo **URL de Entrust**, escriba la URL del servidor de Entrust IdentityGuard.
6. Haga clic en **Agregar**.

Después de terminar:

- Creación de un perfil de certificado de CA para enviar el certificado de CA de Entrust a los dispositivos y asignar el perfil a los mismos usuarios o grupos a los que está asignado el perfil de credenciales del usuario.
- Crear un perfil de credenciales de usuario para utilizar credenciales inteligentes de Entrust en los dispositivos.

Conexión de BlackBerry UEM al software de OpenTrust de la empresa

Para ampliar la autenticación basada en certificados de OpenTrust a los dispositivos, debe agregar una conexión al software de OpenTrust de la empresa. BlackBerry UEM admite la integración con OpenTrust PKI 4.8.0 y posteriores y OpenTrust CMS 2.0.4 y posteriores. Esta conexión no es compatible con aplicaciones BlackBerry Dynamics.

Antes de empezar: Póngase en contacto con el administrador de OpenTrust de la empresa para obtener la URL del servidor de OpenTrust, el certificado por parte del cliente que contiene la clave privada (formato .pfx o .p12) y la contraseña del certificado.

1. En la barra de menús, haga clic en **Configuración**.
2. Haga clic en **Integración externa > Autoridad de certificación**.
3. Haga clic en **Agregar una conexión OpenTrust**.
4. En el campo **Nombre de la conexión**, escriba un nombre para la conexión.
5. En el campo **URL**, escriba la URL del software de OpenTrust.
6. Haga clic en **Examinar**. Desplácese y seleccione el certificado por parte del cliente que puede utilizar BlackBerry UEM para autenticar la conexión al servidor de OpenTrust.
7. En el campo **Contraseña del certificado**, escriba la contraseña del certificado del servidor de OpenTrust.
8. Para probar la conexión, haga clic en **Probar conexión**.
9. Haga clic en **Guardar**.

Después de terminar:

- Cree un perfil de credenciales de usuario para enviar certificados de su software de PKI a los dispositivos.
- Cuando se utiliza la conexión de BlackBerry UEM con el software de OpenTrust para distribuir certificados a los dispositivos, puede haber un breve retraso en la validez de los certificados. Este retraso podría causar problemas con la autenticación de correo durante el proceso de activación del dispositivo. Para resolver este problema, en el software de OpenTrust, configure la CA de OpenTrust y establezca "Retrasar fecha de certificados (segundos)" en 180.

Conexión de BlackBerry UEM a un conector PKI de BlackBerry Dynamics

Si desea utilizar el software PKI de su empresa para la inscripción de certificados para las aplicaciones BlackBerry Dynamics y su software PKI no es compatible con una conexión directa con BlackBerry UEM, puede configurar un conector PKI de BlackBerry Dynamics para comunicarse con su CA y vincular BlackBerry UEM con el conector PKI.

Nota: En entornos BlackBerry UEM Cloud, debe tener instalado BlackBerry Connectivity Node para permitir la comunicación de BlackBerry UEM con el conector PKI a través de BlackBerry Cloud Connector.

Un conector de PKI es un conjunto de programas Java y servicios web en un servidor backend que permite a BlackBerry UEM enviar solicitudes de certificado y recibir las respuestas de la CA. BlackBerry UEM utiliza el protocolo de gestión de certificados de usuario de BlackBerry Dynamics para comunicarse con el conector de PKI. Este protocolo se ejecuta a través de HTTPS y define los mensajes con formato JSON. Para obtener más información sobre la configuración de un conector de PKI de BlackBerry Dynamics, consulte la documentación de Protocolo de gestión de certificados de usuario y conector de PKI.

Antes de empezar: Configure un conector de PKI de BlackBerry Dynamics.

1. En la barra de menús, haga clic en **Configuración > Integración externa > Autoridad de certificación**.
2. Haga clic en **Agregar una conexión de PKI de BlackBerry Dynamics**.
3. En el campo **Nombre de la conexión**, escriba un nombre para la conexión.
4. En el campo **URL**, escriba la URL del conector de PKI.
5. Seleccione una de las siguientes opciones:
   - **Autenticar con nombre de usuario y contraseña**: elija esta opción si BlackBerry UEM se autentica con el conector de PKI de BlackBerry Dynamics mediante la autenticación basada en contraseña.
   - **Autenticar con certificado de cliente**: elija esta opción si BlackBerry UEM se autentica con el conector de PKI de BlackBerry Dynamics mediante la autenticación basada en certificado.
6. Si ha seleccionado **Autenticar con nombre de usuario y contraseña**, en los campos **Nombre de usuario** y **Contraseña**, escriba el nombre de usuario y la contraseña del conector de PKI de BlackBerry Dynamics.
7. Si ha seleccionado **Autenticar con certificado de cliente**, haga clic en **Examinar** para seleccionar y cargar un certificado que sea de confianza para el conector de PKI de BlackBerry Dynamics. En el campo **Contraseña del certificado de cliente**, escriba la contraseña del certificado.
8. En la sección **Certificado de confianza para el conector PKI** puede especificar el certificado que utiliza BlackBerry UEM para establecer conexiones de confianza con el conector PKI, seleccione una de las siguientes opciones:
   - **Certificado de CA de BlackBerry Control TrustStore**
   - **Certificado de CA**: si selecciona esta opción, deberá hacer clic en Examinar para seleccionar el certificado de CA de la empresa.

- **Certificado de servidor de conector PKI**: si selecciona esta opción, deberá hacer clic en Examinar para seleccionar el certificado de servidor de conector PKI de la empresa.

9. Para probar la conexión, haga clic en **Probar conexión**.
10. Haga clic en **Guardar**.

Después de terminar:

- Cree un perfil de credenciales de usuario para enviar certificados de su software de PKI a los dispositivos.

Conexión de BlackBerry UEM a la solución PKI basada en aplicación de su empresa

Las soluciones PKI basadas en aplicación, como Purebred, incluyen una aplicación instalada en un dispositivo que se comunica con una CA para inscribir certificados y agregarlos al dispositivo. Puede utilizar una solución PKI basada en aplicación para proporcionar certificados para su uso en las aplicaciones de BlackBerry Dynamics.

Para utilizar una solución PKI basada en aplicación con dispositivos iOS, debe agregar una conexión entre BlackBerry UEM y el proveedor de PKI. Esta tarea no es necesaria para utilizar una solución PKI basada en aplicación solo con dispositivos Android.

Si la aplicación PKI que recupera los certificados de la CA no es una aplicación de BlackBerry Dynamics, BlackBerry UEM Client se comunica con la aplicación PKI para obtener los certificados y proporcionárselos a las aplicaciones de BlackBerry Dynamics.

Antes de empezar: Verifique que la aplicación que recupera los certificados para su uso en las aplicaciones de BlackBerry Dynamics se encuentra en la lista de aplicaciones en BlackBerry UEM.

1. En la barra de menú, haga clic en **Configuración > Integración externa > Autoridad de certificación**.
2. Haga clic en **Añadir una conexión para los certificados basados en dispositivo**.
3. Seleccione la aplicación que recupera los certificados de la aplicación PKI para su uso en las aplicaciones de BlackBerry Dynamics. Para utilizar Purebred, seleccione BlackBerry UEM Client.
4. Haga clic en **Agregar**.

Después de terminar:

- Creación de perfiles de credenciales de usuario para certificados basados en aplicaciones.
- Creación de un perfil de credenciales de usuario para usar certificados basados en aplicaciones en dispositivos iOS.
- Creación de un perfil de credenciales de usuario para utilizar certificados del almacén de claves nativo

Integración de certificados de cliente en dispositivos y aplicaciones

Tanto usted como los usuarios pueden enviar los certificados de cliente a los dispositivos y las aplicaciones de varias maneras:

Cómo se agrega el certificado	Descripción	Dispositivos compatibles
Durante la activación del dispositivo	BlackBerry UEM envía los certificados a los dispositivos durante el proceso de activación. Los dispositivos utilizan estos certificados para establecer conexiones seguras entre el dispositivo y BlackBerry UEM.	Todas
Perfiles SCEP	Puede crear perfiles SCEP que los dispositivos pueden utilizar para conectarse y obtener certificados de cliente de la CA de su empresa mediante un servicio SCEP. Los dispositivos y aplicaciones BlackBerry Dynamics pueden utilizar estos certificados para realizar la autenticación basada en certificados y para conectarse a la red Wi-Fi, la VPN y el servidor de correo del trabajo.	iOS macOS Android Windows 10
Conexión a la solución de PKI de la empresa	Si su empresa utiliza una solución de PKI, como los productos de software de Entrust o OpenTrust para emitir y gestionar certificados, puede crear perfiles de credenciales de usuario que los dispositivos pueden utilizar para obtener certificados de cliente de la CA de su empresa. Los dispositivos con BlackBerry Dynamics utilizan estos certificados para la autenticación basada en certificados de las aplicaciones de BlackBerry Dynamics. Otros dispositivos utilizan estos certificados para realizar la autenticación basada en certificados desde el navegador y para conectarse a la red Wi-Fi, la VPN y el servidor de correo del trabajo.	iOS (macOS solo para BlackBerry Access) Android (Windows 10 solo para BlackBerry Access)
Perfiles de certificado compartido	Los perfiles de certificado compartido especifican el certificado de cliente que BlackBerry UEM envía a los dispositivos iOS, macOS y Android. BlackBerry UEM envía el mismo certificado de cliente a todos los usuarios a los que se ha asignado el perfil. El administrador debe tener acceso al certificado y la clave privada para crear un perfil de certificado compartido.	iOS macOS Android

Cómo se agrega el certificado	Descripción	Dispositivos compatibles
Envío de certificados de cliente a cuentas de usuario individuales	Puede agregar un certificado de cliente a una cuenta de usuario. BlackBerry UEM puede enviar el certificado a los dispositivos iOS y Android del usuario. Si el certificado se asocia con un perfil de credenciales de usuario, los dispositivos pueden utilizar estos certificados para conectarse a su red Wi-Fide trabajo, VPN de trabajo y servidor de correo de trabajo. El administrador debe tener acceso al certificado y la clave privada para enviar el certificado del cliente al usuario.	iOS Android
Carga de usuarios en UEM Self-Service	Si su empresa tiene un entorno local de BlackBerry UEM, los usuarios pueden cargar certificados en BlackBerry UEM Self-Service. A continuación, BlackBerry UEM inserta el certificado en los dispositivos de los usuarios. Si el certificado se asocia con un perfil de credenciales de usuario, los dispositivos y las aplicaciones BlackBerry Dynamics pueden utilizar estos certificados para una autenticación basada en certificados y para conectarse a su red Wi-Fi de trabajo, VPN de trabajo y servidor de correo de trabajo. Esta función no es compatible en BlackBerry UEM Cloud.	iOS Android
Importación por parte de los usuarios	En los dispositivos con BlackBerry 10, los usuarios pueden importar los certificados de cliente al almacén de certificados del dispositivo en la sección "Seguridad y privacidad" de "Configuración del sistema". Los certificados que se van a utilizar en el navegador de trabajo o bien para enviar mensajes protegidos con S/MIME desde la cuenta de correo de trabajo pueden importarse desde el sistema de archivos en el dispositivo o desde una ubicación de red a la que se puede acceder desde el espacio de trabajo. En los dispositivos con Android, los usuarios pueden agregar certificados al almacén de claves nativo para su uso con las aplicaciones BlackBerry Dynamics.	Android

Envío de certificados a dispositivos y aplicaciones mediante perfiles

Puede enviar certificados a los dispositivos y aplicaciones utilizando los siguientes perfiles disponibles en la biblioteca Políticas y perfiles:

Perfil	Descripción
Certificado de CA	Los perfiles de certificado de CA especifican un certificado de CA que los dispositivos y aplicaciones BlackBerry Dynamics pueden utilizar para confiar en la identidad asociada con cualquier certificado de cliente o servidor que la CA haya firmado.
Credencial de usuario	Los perfiles de credenciales de usuario envían certificados a los dispositivos de las siguientes formas: • Pueden especificar una conexión al software de PKI de su empresa para enviar certificados de cliente a los dispositivos y aplicaciones BlackBerry Dynamics. • Pueden permitirle cargar manualmente certificados en BlackBerry UEM y, en un entorno local, permitir que los usuarios carguen certificados utilizando BlackBerry UEM Self-Service. • Pueden permitir que las aplicaciones BlackBerry Dynamics en dispositivos con Android y la aplicación BlackBerry Access estén activados que los dispositivos macOS y Windows 10 utilicen certificados desde el almacén de claves nativo. • Pueden permitir que las aplicaciones BlackBerry Dynamics importen certificados desde otras soluciones PKI basadas en aplicaciones como Purebred.
SCEP	Los perfiles SCEP especifican cómo los dispositivos y aplicaciones de BlackBerry Dynamics se conectan a la CA de la empresa y obtienen certificados de clientes de esta mediante un servicio SCEP.
Certificado compartido	Los perfiles de certificado compartido especifican un certificado de cliente que BlackBerry UEM envía a los dispositivos iOS y Android. BlackBerry UEM envía el mismo certificado de cliente a todos los usuarios a los que se ha asignado el perfil.

Para los dispositivos iOS y Android, también puede enviar un certificado de cliente a un dispositivo agregándolo directamente a una cuenta de usuario. Para obtener más información, consulte Adición de un certificado de cliente a una cuenta de usuario.

Para los dispositivos con iOS y Android, si la empresa utiliza certificados de S/MIME, también puede usar perfiles para permitir que los dispositivos puedan obtener claves públicas del destinatario y comprobar el estado del certificado. Para obtener más información, consulte Ampliación de la seguridad del correo mediante S/MIME.

Para que las aplicaciones de BlackBerry Dynamics utilicen certificados enviados por perfiles, debe seleccionar "Permitir que las aplicaciones de BlackBerry Dynamics utilicen certificados de usuario, perfiles SCEP y perfiles de credenciales de usuario" en la configuración de la aplicación.

Elección de perfiles para enviar certificados de cliente a los dispositivos y las aplicaciones

Puede utilizar diferentes tipos de perfiles para enviar certificados de cliente a los dispositivos y aplicaciones BlackBerry Dynamics. El tipo de perfil que seleccione dependerá de cómo su empresa utilice los certificados y los tipos de dispositivos que admita la empresa. Considere las siguientes directrices:

- Para utilizar perfiles SCEP, debe tener una CA que admita SCEP.
- Si ha configurado una conexión entre BlackBerry UEM y la solución PKI de la empresa, utilice los perfiles de credenciales de usuario para enviar certificados a los dispositivos. Puede conectarse directamente a una CA de Entrust o CA de OpenTrust. También puede utilizar un conector de PKI de BlackBerry Dynamics para conectarse a un servidor CA a fin de inscribir certificados para dispositivos con BlackBerry Dynamics.
- Para utilizar certificados con aplicaciones de BlackBerry Dynamics, debe utilizar un perfil de credenciales de usuario o agregar certificados a cuentas de usuario individuales.
- Para permitir que los usuarios carguen certificados que puedan utilizar para conectarse a su red Wi-Fi de trabajo, red VPN de trabajo y servidor de correo del trabajo, utilice un perfil de credenciales de usuario.
- Para utilizar certificados de cliente para Wi-Fi, VPN y autenticación del servidor de correo, debe asociar el perfil de certificado con un perfil Wi-Fi, VPN o de correo electrónico.

  Nota: Los dispositivos Android Enterprise no son compatibles con el uso de los certificados que BlackBerry UEM ha enviado a los dispositivos para la autenticación Wi-Fi.
- Los perfiles de certificado compartido y los perfiles que agrega a las cuentas de usuario no mantienen la clave privada en privado porque se debe tener acceso a ella. La conexión a un CA mediante perfiles de credenciales de usuario o SCEP es más segura porque la clave privada solo se envía al dispositivo para el que se emitió el certificado.

Envío de certificados de CA a dispositivos y aplicaciones

Es posible que necesite distribuir certificados de CA en los dispositivos si la empresa utiliza S/MIME o si los dispositivos o las aplicaciones de BlackBerry Dynamics utilizan autenticación basada en certificados para conectarse a una red o servidor en el entorno de la empresa.

Cuando se almacena un certificado de CA en un dispositivo, el dispositivo y las aplicaciones confían en la identidad asociada a cualquier certificado de cliente o servidor firmado por la CA. Cuando el certificado de la CA que ha firmado los certificados de red y servidor de la empresa se guarda en los dispositivos, el dispositivo y las aplicaciones pueden confiar en sus redes y servidores al establecer conexiones seguras. Cuando el certificado de la CA que ha firmado los certificados S/MIME de la empresa se guarda en los dispositivos, el cliente de correo electrónico puede confiar en el certificado del remitente al recibir un mensaje de correo seguro.

Varios de los certificados de CA que se utilizan con distintos fines se pueden guardar en un dispositivo. Puede utilizar perfiles de certificados de CA para enviar certificados de CA a los dispositivos.

Creación de un perfil de certificado de CA

Antes de empezar: Obtenga el archivo de certificado de CA del administrador de PKI.

1. En la barra de menú, haga clic en **Políticas y perfiles**.
2. Haga clic en **Certificados > Certificado de CA**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil. Cada perfil de certificado de CA debe tener un nombre único. Algunos nombres (por ejemplo, ca_1) están reservados.

5. En el campo **Archivo de certificado**, haga clic en **Examinar** para ubicar el archivo de certificado.
6. Si el certificado de CA se envía a los dispositivos con BlackBerry 10, en la pestaña BlackBerry, especifique uno o más de los siguientes almacenes de certificados para enviar el certificado al dispositivo:
   - Almacén de certificados del navegador
   - Almacén de certificados de VPN
   - Almacén de certificados de Wi-Fi
   - Almacén de certificados de empresa
7. Si el certificado CA se envía a los dispositivos macOS, en la pestaña macOS, en la lista desplegable **Aplicar perfil a**, seleccione **Usuario** o **Dispositivo**.
8. Haga clic en **Agregar**.

Envío de certificados de cliente a dispositivos y aplicaciones mediante perfiles de credenciales de usuario

Los perfiles de credenciales de usuario permiten que los dispositivos utilicen certificados de cliente obtenidos mediante los métodos siguientes:

- Carga manual de certificados a la consola de administración de BlackBerry UEM o, en un entorno local, a BlackBerry UEM Self-Service
- Una conexión establecida entre BlackBerry UEM y la CA de Entrust o la CA de OpenTrust de su empresa
- Para aplicaciones de BlackBerry Dynamics en dispositivos con Android, certificados almacenados en el almacén de claves nativo del dispositivo
- Para aplicaciones de BlackBerry Dynamics, a través de una conexión establecida con el conector de PKI de BlackBerry Dynamics
- Para aplicaciones de BlackBerry Dynamics, utilizando una solución PKI basada en aplicación, como Purebred.

Si los usuarios cargan los certificados manualmente en UEM Self-Service, puede ver el certificado en la página de usuario de la consola de gestión. También puede eliminar o sustituir el certificado. Esta función no es compatible en BlackBerry UEM Cloud.

Los perfiles de credenciales de usuario son compatibles con los dispositivos con iOS y Android. Las soluciones PKI basadas en aplicación son compatibles con aplicaciones de BlackBerry Dynamics en iOS y dispositivos Android. La carga manual de certificados es compatible en iOS, Android Enterprise, y Samsung Knox Workspace.

Para obtener más información sobre la conexión de BlackBerry UEM al software de PKI de su empresa, consulte Integración de BlackBerry UEM con el software PKI de la empresa.

De manera alternativa, puede utilizar perfiles SCEP para inscribir los certificados de cliente en los dispositivos. También puede cargar certificados directamente en una cuenta de usuario. El tipo de perfil que seleccione dependerá de cómo su empresa utilice el software PKI, los tipos de dispositivos que admita la empresa y cómo desee administrar certificados.

Cree un perfil de credenciales de usuario para cargar manualmente los certificados

Los perfiles de credenciales de usuario permiten cargar manualmente un certificado que se enviará a los dispositivos del usuario.

1. En la barra de menú, haga clic en **Políticas y perfiles**.
2. Haga clic en **Certificados > Credenciales de usuario**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil. Cada perfil de certificado debe tener un nombre único.

5. En la lista desplegable **Conexión con la autoridad de certificación**, seleccione **Certificado cargado manualmente**.
6. Si está administrando dispositivos Android Enterprise y desea evitar que los usuarios seleccionen el certificado para utilizarlo con otros fines, en la pestaña **Android** seleccione **Ocultar certificado en dispositivos Android Enterprise**. Esta configuración se aplica únicamente a dispositivos con Android 9.0 o versiones posteriores.
7. Haga clic en **Agregar**.

Después de terminar:

- Si los dispositivos utilizan los certificados de cliente para autenticarse con una red Wi-Fi, una VPN o un servidor de correo, asocie el perfil de credenciales de usuario a un perfil Wi-Fi, de VPN o de correo.
- Asigne el perfil a las cuentas de usuario y los grupos de usuarios.
- Adición de un certificado de cliente a un perfil de credenciales de usuario o indique a los usuarios que utilicen BlackBerry UEM Self-Service para cargar su propio certificado.

Creación de un perfil de credenciales de usuario para conectarse al software de PKI de su empresa

Los perfiles de credenciales de usuario que se conectan al software de PKI de la empresa pueden inscribir certificados para dispositivos con iOS y Android. Si la conexión se realiza con el software de PKI de Entrust, el perfil de credenciales de usuario también puede inscribir certificados para aplicaciones de BlackBerry Dynamics.

Nota: BlackBerry UEM no es compatible con el historial de claves de los certificados emitidos para las aplicaciones de BlackBerry Dynamics.

Antes de empezar:

- Configure una conexión al software de Entrust o OpenTrust de su empresa.
- Contacte con el administrador de Entrust o de OpenTrust de la empresa para confirmar qué perfil de PKI debe seleccionar. BlackBerry UEM obtiene una lista de perfiles del software PKI.
- Solicite al administrador de Entrust o OpenTrust los valores para el perfil que debe proporcionar. Por ejemplo, los valores del tipo de dispositivo (devicetype), grupo de Entrust IdentityGuard (iggroup) y nombre de usuario de Entrust IdentityGuard (igusername).
- Si el sistema OpenTrust de su empresa está configurado para devolver solo claves bajo custodia, el administrador de OpenTrust debe verificar que haya certificados para cada usuario en el sistema OpenTrust. Al asignar un perfil de credenciales de usuario a los usuarios en BlackBerry UEM no se crean automáticamente certificados para usuarios en OpenTrust. En este caso, un perfil de credenciales de usuario solo puede distribuir certificados a los usuarios que tienen un certificado existente en el sistema OpenTrust.

1. En la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Certificados > Credenciales de usuario**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil. Cada perfil de certificado debe tener un nombre único.
5. En la lista desplegable **Conexión con la autoridad de certificación**, seleccione la conexión de Entrust o OpenTrust que configuró.
6. En la lista desplegable **Perfil**, haga clic en el perfil adecuado.
7. Especifique los valores para el perfil.
8. Si es necesario, puede especificar un tipo de SAN y un valor para un certificado de cliente de Entrust.
   a) En la tabla de SAN, haga clic en +.
   b) En la lista desplegable **Tipo de SAN**, haga clic en el tipo adecuado.
   c) En el campo **Valor de SAN**, escriba el valor de SAN.

   Si se establece el tipo de SAN en "Nombre de RFC822", el valor debe ser una dirección de correo válida. Si se establece en "URI", el valor debe ser una URL válida que incluya el protocolo y la dirección IP o FQDN. Si

se establece en "Nombre principal de NT", el valor debe ser un nombre principal válido. Si se establece en "Nombre de DNS", el valor debe ser un FQDN válido.

9. Especifique el **Período de renovación** del certificado. El periodo puede ser entre 1 y 120 días.
10. Haga clic en **Agregar**.

Después de terminar:

- Si los dispositivos utilizan los certificados de cliente para autenticarse con una red Wi-Fi, una VPN o un servidor de correo, asocie el perfil de credenciales de usuario a un perfil Wi-Fi, de VPN o de correo.
- Asigne el perfil a las cuentas de usuario y los grupos de usuarios. Se les solicita a los usuarios de Android que introduzcan una contraseña cuando reciben el perfil (la contraseña se muestra en pantalla).

Crear un perfil de credenciales de usuario para utilizar credenciales inteligentes de Entrust en los dispositivos

Las credenciales inteligentes derivadas de Entrust son compatibles con las siguientes aplicaciones:

- Aplicaciones de BlackBerry Dynamics en dispositivosiOS
- Aplicaciones de BlackBerry Dynamics en dispositivos Android que no sean dispositivos Samsung Knox Workspace
- Aplicaciones en dispositivos Android Enterprise que utilizan certificados para firma, cifrado y autenticación de identidad, como BlackBerry Hub y los navegadores web compatibles
- Aplicaciones en dispositivos Samsung Knox Workspace que utilizan certificados para firma, cifrado y autenticación de identidad, como el cliente de correo nativo de Samsung y los navegadores web compatibles

Nota: BlackBerry UEM no es compatible con el historial de claves para credenciales inteligentes derivadas.

Antes de empezar:

- Conectar BlackBerry UEM al servidor de Entrust IdentityGuard de su empresa para utilizar credenciales inteligentes.
- Creación de un perfil de certificado de CA para enviar el certificado de CA de Entrust a los dispositivos y asignar el perfil a los mismos usuarios o grupos a los que está asignado este perfil de credenciales del usuario.

1. En la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Certificados > Credenciales de usuario**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil. Cada perfil de certificado debe tener un nombre único.
5. En la lista desplegable **Conexión con la autoridad de certificación**, seleccione la conexión de credenciales inteligentes de Entrust que ha configurado.
6. En la lista desplegable **Tipo de certificado**, especifique si la credencial inteligente se utilizará para autenticación de identidad, firma o cifrado.

   Si desea enviar credenciales inteligentes a aplicaciones para más de un fin, cree perfiles de credenciales de usuario adicionales.
7. Si la credencial inteligente se enviará a dispositivos Samsung Knox Workspace o a aplicaciones que no sean las aplicaciones de BlackBerry Dynamics en dispositivos Android Enterprise, haga clic en la pestaña **Android** y seleccione **Entregar a llavero nativo**.

   Si no se selecciona esta opción, solo las aplicaciones de BlackBerry Dynamics pueden utilizar la credencial inteligente.
8. Si la credencial inteligente se enviará a aplicaciones de BlackBerry Dynamics, haga clic en la pestaña **BlackBerry Dynamics** y lleve a cabo las acciones siguientes:

a) Si desea permitir que los usuarios descarten la inscripción de certificados y la completen más adelante, seleccione **Permitir inscripción de certificados opcional**. La inscripción de certificados opcional es compatible con dispositivos con iOS y Androidpara los siguientes tipos de perfiles de credenciales de usuario: proveedor basado en dispositivos (aplicación), credencial inteligente de confianza y almacén de claves nativo.
b) Si desea que el dispositivo elimine credenciales duplicadas, seleccione **Eliminar certificados duplicados**. El dispositivo elimina la credencial que tiene la fecha de inicio más inmediata.
c) Si desea que el dispositivo elimine credenciales caducadas, seleccione **Eliminar certificados caducados**.
d) Para permitir que todas las aplicaciones de BlackBerry Dynamics utilicen las credenciales inteligentes, seleccione **Permitir que todas las aplicaciones utilicen certificados**.
e) Para especificar las aplicaciones de BlackBerry Dynamics que utilizan las credenciales inteligentes, seleccione **Permitir que aplicaciones específicas utilicen certificados** ya haga clic en + para especificar las aplicaciones. Debe incluir BlackBerry UEM Client en la lista de aplicaciones.

9. Haga clic en **Agregar**.

Después de terminar:

- Asigne el perfil a las cuentas de usuario y los grupos de usuarios.
- Después de que un dispositivo reciba el perfil, los usuarios deben iniciar sesión en el módulo de autoservicio de Entrust IdentityGuard para activar su credencial inteligente y utilizar BlackBerry UEM Client para escanear el código QR presentado por el módulo de autoservicio de Entrust IdentityGuard y agregar la credencial inteligente al dispositivo.
- Para eliminar una credencial inteligente de Entrust de un dispositivo, el usuario debe desactivar la credencial inteligente en BlackBerry UEM Client antes de anular la asignación del perfil o eliminar el certificado.

Creación de un perfil de credenciales de usuario para utilizar certificados del almacén de claves nativo

Puede configurar el perfil de credenciales de usuario para utilizar certificados del almacén de claves nativo en las siguientes situaciones:

- Para permitir que las aplicaciones de BlackBerry Dynamics utilicen un certificado del almacén de claves nativo en dispositivos con Android
- Para permitir que las aplicaciones de BlackBerry Dynamics utilicen un certificado desde el almacén de claves nativo para acceder a tokens criptográficos desde aplicaciones PKI en dispositivos con iOS
- Para permitir que la aplicación de BlackBerry Access utilice un certificado del almacén de claves nativo en dispositivos con macOS o con Windows 10

Puede permitir que las aplicaciones utilicen cualquier certificado que se haya añadido al almacén de claves o definir restricciones de los certificados que puede escoger la aplicación. Por ejemplo, si está utilizando una solución PKI basada en aplicación como Purebred, que añade certificados al almacén de claves nativo, puede forzar la aplicación para que seleccione un certificado emitido por su solución PKI Purebred y obligar a que la aplicación utilice certificados con capacidades específicas.

Nota: "Almacén de claves nativo" hace referencia al almacén de claves del dispositivo. Todos los perfiles de credenciales del usuario con conectores del almacén de claves nativo deben asignarse al usuario antes de comenzar a detectar certificados. Si un certificado cumple con los requisitos de más de un UCP, se optará por la mejor coincidencia.

1. En la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Certificados > Credenciales de usuario**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil. Cada perfil de certificado debe tener un nombre único.
5. En la lista desplegable **Conexión con la autoridad de certificación**, seleccione **Almacén de claves nativo**.

6. En la sección **Plataformas compatibles**, seleccione los tipos de SO del dispositivo que desea que este perfil admita.
7. En la sección **Inscripción de certificados**, seleccione **Permitir inscripción de certificados opcional** si desea permitir que los usuarios descarten la inscripción de certificados y la completen más tarde.

   Esto se aplica solo a dispositivos con Android.
8. Para especificar qué certificado utilizará la aplicación de BlackBerry Dynamics, realice las acciones siguientes:
   a) Junto a **Emisores**, haga clic en + y escriba el nombre del emisor.

      Las aplicaciones de BlackBerry Dynamics solo utilizarán un certificado si el emisor especificado coincide con el OID abreviado de OpenSSL en el certificado. Puede copiar este valor del certificado del emisor. No incluya espacios antes o después del signo igual (=). Por ejemplo:

      ```
      CN=Acme_cert SMIME,OU=Acme_Legal,O=Acme,C=Can
                                CN=Acme_cert SMIME,OU=Acme_Legal,O=Acme
                                CN=Acme_cert TLS
      ```
   b) En la sección **Uso de la clave**, seleccione las operaciones con las que es compatible el certificado.

      Las aplicaciones de BlackBerry Dynamics solo utilizarán certificados en los que se haya especificado al menos el valor de uso de la clave. Por ejemplo, un certificado de cifrado puede tener un valor de uso de la clave de **Cifrado de clave**. Un certificado de autenticación puede tener un valor de uso de la clave de **Firma digital**. Un certificado de firma puede tener un valor de uso de la clave de **Firma digital** y **No rechazo**.
   c) En la sección **Uso extendido de la clave**, seleccione las funciones para las que se emitió el certificado.

      Las aplicaciones de BlackBerry Dynamics solo utilizarán certificados si todos los valores de uso de la clave ampliados seleccionados están presentes en el certificado. Los certificados pueden tener más valores de uso de la clave ampliados.
   d) Si el certificado se emitió para fines distintos al uso en correo electrónico, la autenticación de cliente y el inicio de sesión con tarjeta inteligente, seleccione **Uso de ID de objeto adicional**, haga clic en + y especifique el OID del uso de la clave. Por ejemplo, si el certificado se va a utilizar para autenticación de servidor, puede tener el OID 1.3.6.1.5.5.7.3.1
9. Si desea que el dispositivo elimine certificados caducados, seleccione **Eliminar certificados caducados**.

   Los certificados de cifrado caducados utilizados para S/MIME deben conservarse en el dispositivo para que los usuarios puedan leer los mensajes cifrados antes de la caducidad del certificado de cifrado.
10. Si desea que el dispositivo elimine certificados duplicados, seleccione **Eliminar certificado duplicado**. El dispositivo elimina el certificado que tiene la fecha de inicio más inmediata.
11. Haga clic en **Agregar**.

Después de terminar:

- Permita que las aplicaciones de BlackBerry Dynamics usen certificados.
- Asigne el perfil a las cuentas de usuario y los grupos de usuarios.

Creación de un perfil de credenciales de usuario para conectarse al conector de PKI de BlackBerry Dynamics

1. En la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Certificados > Credenciales de usuario**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil. Cada perfil de certificado debe tener un nombre único.
5. En la lista desplegable **Conexión con la autoridad de certificación**, seleccione la conexión de PKI de BlackBerry Dynamics que haya configurado.

6. Si el usuario debe proporcionar una contraseña para solicitar un certificado, seleccione **Requerir contraseña introducida por el usuario u OTP**.
7. Si desea permitir que el dispositivo solicite automáticamente un nuevo certificado antes de que el certificado actual caduque, seleccione **Activar la renovación de certificados** y especifique el número de días previos a la caducidad en que los dispositivos deben solicitar un nuevo certificado.
8. Si desea que el dispositivo elimine certificados caducados, seleccione **Eliminar certificados caducados**.
9. Si desea que el dispositivo elimine certificados duplicados, seleccione **Eliminar certificado duplicado**. El dispositivo elimina el certificado que tiene la fecha de inicio más inmediata.
10. Haga clic en **Agregar**.

Después de terminar:

- Permita que las aplicaciones de BlackBerry Dynamics usen certificados.
- Asigne el perfil a las cuentas de usuario y los grupos de usuarios.
- Si actualiza el conector PKI, haga clic en **Actualizar capacidades de PKI** para actualizar las funciones PKI admitidas para el perfil.

Renovación de certificados que están escritos mediante el conector de PKI de BlackBerry Dynamics

Si necesita actualizar los certificados de usuario de todos los usuarios de BlackBerry Dynamics, puede enviar un comando para solicitar la renovación de los certificados a todos los dispositivos que tengan asignado el perfil de credenciales de usuario.

1. En la barra de menú, haga clic en **Políticas y perfiles**.
2. Haga clic en **Certificados > Credenciales de usuario**.
3. Haga clic en el nombre del perfil que desea cambiar.
4. Haga clic en **Actualizar capacidades de PKI** para asegurarse de que BlackBerry UEM tiene los detalles más recientes del conector de PKI.
5. Haga clic en **Renovar** para ordenar a todos los dispositivos con BlackBerry Dynamics que tengan asignado el perfil que soliciten la renovación de certificados.

Creación de perfiles de credenciales de usuario para certificados basados en aplicaciones

Las soluciones PKI basadas en aplicación, como Purebred, incluyen una aplicación instalada en un dispositivo que se comunica con una CA para inscribir certificados y agregarlos al dispositivo. Puede utilizar una solución PKI basada en aplicación para proporcionar certificados para su uso en las aplicaciones de BlackBerry Dynamics.

Para utilizar una solución PKI basada en aplicación con dispositivos iOS, debe agregar una conexión entre BlackBerry UEM y el proveedor de PKI. Esta tarea no es necesaria para utilizar una solución PKI basada en aplicación solo con dispositivos Android.

Si la aplicación PKI que recupera los certificados de la CA no es una aplicación de BlackBerry Dynamics, BlackBerry UEM Client se comunica con la aplicación PKI para obtener los certificados y proporcionárselos a las aplicaciones de BlackBerry Dynamics.

Si envía más de un certificado a los dispositivos con este método, es recomendable que configure varios perfiles de credenciales de usuario e incluya un tipo diferente de certificado en cada perfil. Si utiliza una sola instancia de perfil para varios certificados, no hay indicación en caso de que falten certificados. Por ejemplo, si un perfil incluye certificados independientes de cifrado, firma y autenticación y solo se importan los certificados de firma y autenticación, en el dispositivo parece que la información se ha realizado correctamente aunque falte el certificado de cifrado. Sin embargo, si configura tres perfiles de credenciales de usuario independientes y falta el certificado de cifrado, el problema se hará evidente.

Pasos que deberá seguir para la utilización de certificados basados en aplicaciones

Algunos de los pasos requeridos para utilizar la solución PKI basada en aplicaciones de su empresa solo resultan necesarios si utiliza la solución con dispositivos iOS.

Paso	Acción
1	Para utilizar una solución de PKI basada en aplicaciones con dispositivos iOS, en el perfil de BlackBerry Dynamics seleccione **Activar UEM Client para que pueda inscribirse en BlackBerry Dynamics** y designe BlackBerry UEM Client para **Delegación de autenticación de aplicaciones**.
2	Para utilizar una solución de PKI basada en aplicaciones con dispositivos iOS, conecte BlackBerry UEM a la solución de PKI basada en aplicaciones de su empresa.
3	Para utilizar una solución de PKI basada en aplicaciones con dispositivos iOS, si la aplicación de PKI no es una aplicación BlackBerry Dynamics, configure BlackBerry UEM Client para que admita certificados basados en aplicaciones.
4	Configuración de las aplicaciones de BlackBerry Dynamics para utilizar certificados basados en aplicación.
5	Asegúrese de que la aplicación PKI (por ejemplo, Purebred) está instalada en los dispositivos de los usuarios.
6	Para utilizar la solución de PKI basada en aplicaciones con dispositivos iOS, cree un perfil de credenciales de usuario para usar los certificados basados en aplicaciones.
7	Para utilizar una solución de PKI basada en aplicaciones con dispositivos Android, cree un perfil de credenciales de usuario para usar los certificados del almacén de claves nativo.

Configuración de BlackBerry UEM Client para que sea compatible con certificados basados en aplicación

Esta tarea solo es necesaria si utiliza la solución de PKI basada en aplicación de su empresa con dispositivos con iOS y la aplicación de PKI no es una aplicación de BlackBerry Dynamics.

1. En la consola de administración de BlackBerry UEM, haga clic en la opción **Aplicaciones** de la barra de menú.
2. En la lista de aplicaciones, seleccione BlackBerry UEM Client.
3. En la sección Configuración de aplicación, haga clic en +.
4. En el campo **Nombre de aplicación**, escriba un nombre para la aplicación.
5. En el campo **UTI schemes**, especifique los esquemas de UTI de la solución PKI basada en aplicación de su empresa. Por ejemplo, si utiliza la aplicación de Purebred, deberá utilizar los siguientes esquemas: `purebred.select.all-user`, `purebred.select.no-filter`, `purebred.zip.all-user`, `purebred.zip.no-filter`.
6. Haga clic en **Guardar**.
7. Asigne BlackBerry UEM Client con la configuración de aplicación que ha creado a los usuarios y dispositivos que desea que utilicen la solución PKI basada en aplicación.

Configuración de las aplicaciones de BlackBerry Dynamics para utilizar certificados basados en aplicación

Las aplicaciones de BlackBerry Dynamics seleccionan automáticamente el certificado que se usará para S/MIME y para la autenticación a través de conexiones TLS basadas en las propiedades del uso de la clave y el uso extendido de esta en los certificados. Si dos certificados o más comparten el mismo conjunto de propiedades, las aplicaciones podrían no ser capaces de resolver qué certificado usar para la autenticación de TLS. Los siguientes pasos pueden ayudar a las aplicaciones a determinar el certificado que usar.

1. En la consola de administración de BlackBerry UEM, en la barra de menú, haga clic en **Aplicaciones**.
2. En la lista de aplicaciones, seleccione la aplicación (por ejemplo, BlackBerry Work o BlackBerry Access).
3. Seleccione la opción **Permitir que las aplicaciones de BlackBerry Dynamics utilicen certificados de usuario y perfiles de credenciales de usuario**.
4. Si va a configurar BlackBerry Work, en la sección Configuración de aplicación, haga clic en + y lleve a cabo una de las tareas siguientes:

Tarea	Pasos
Configurar BlackBerry Work cuando su empresa utiliza BEMS	**a.** En la pestaña Configuration Settings, seleccione **Clients must have individual login certificates (SSL) uploaded in the GC**. **b.** Para activar la autodetección del servidor de Microsoft Exchange en el que se encuentran los usuarios, seleccione **Use BEMS to perform Autodiscover of the EAS/EWS endpoint for the user**. **c.** En la pestaña **Exchange Settings**, en el campo **User Credential Profile Name**, escriba del nombre del perfil de credenciales de usuario.
Configurar BlackBerry Work cuando su empresa no utiliza BEMS	**a.** Seleccione la pestaña **Exchange Settings**. **b.** Si el servidor utiliza el formato de inicio de sesión *nombre de dominio\usuario*, en el campo **Dominio predeterminado**, especifique el dominio de Windows NT predeterminado al que se conecta BlackBerry Work cuando los usuarios inician sesión. **c.** En el campo **Active Sync Server**, especifique el servidor de Exchange ActiveSync predeterminado al que BlackBerry Work se conecta cuando los usuarios inician sesión en BlackBerry Work (por ejemplo, cas.mydomain.com). **d.** En el campo **Auto Discover URL**, especifique la URL de autodetección si la sabe. Esto acelera el proceso de configuración de autodetección (por ejemplo, https://autodiscover.mydomain.com). **e.** En el campo **Auto Discover Connection Timeout in Seconds (iOS only)**, especifique el tiempo de espera de conexión de autodetección en segundos. **f.** En el campo **User Credential Profile Name**, escriba del nombre del perfil de credenciales de usuario.

5. Haga clic en **Guardar**.

Creación de un perfil de credenciales de usuario para usar certificados basados en aplicaciones en dispositivos iOS

1. En la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Certificados > Credenciales de usuario**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil. Cada perfil de certificado debe tener un nombre único.

5. En la lista desplegable **Conexión con la autoridad de certificación**, seleccione el nombre de la aplicación que especificó al conectar BlackBerry UEM a su solución PKI. Si utiliza Purebred, seleccione BlackBerry UEM Client
6. Para especificar qué certificado utilizará la aplicación de BlackBerry Dynamics, realice las acciones siguientes:
   a) En la sección **Uso de la clave**, seleccione las operaciones con las que es compatible el certificado.

      Las aplicaciones de BlackBerry Dynamics solo utilizarán certificados en los que se haya especificado al menos el valor de uso de la clave. Por ejemplo, un certificado de cifrado puede tener un valor de uso de la clave de **Cifrado de clave**. Un certificado de autenticación puede tener un valor de uso de la clave de **Firma digital**. Un certificado de firma puede tener un valor de uso de la clave de **Firma digital** y **No rechazo**.
   b) En la sección **Uso extendido de la clave**, seleccione las funciones para las que se emitió el certificado.

      Las aplicaciones de BlackBerry Dynamics solo utilizarán certificados si todos los valores de uso de la clave ampliados seleccionados están presentes en el certificado. Los certificados pueden tener más valores de uso de la clave ampliados.
   c) Si el certificado se emitió para fines distintos al uso en correo electrónico, la autenticación de cliente y el inicio de sesión con tarjeta inteligente, seleccione **Uso de ID de objeto adicional**, haga clic en + y especifique el OID del uso de la clave. Por ejemplo, si el certificado se va a utilizar para autenticación de servidor, puede tener el OID 1.3.6.1.5.5.7.3.1
   d) Junto a **Emisores**, haga clic en + y escriba el nombre del emisor.

      Las aplicaciones de BlackBerry Dynamics solo utilizarán un certificado si el emisor especificado coincide con el OID abreviado de OpenSSL en el certificado. Puede copiar este valor del certificado del emisor. No incluya espacios antes o después del signo igual (=). Por ejemplo:

      ```
      CN=Acme_cert SMIME,OU=Acme_Legal,O=Acme,C=Can
                                          CN=Acme_cert SMIME,OU=Acme_Legal,O=Acme
                                          CN=Acme_cert TLS
      ```
7. Si desea que el dispositivo elimine certificados caducados, seleccione **Eliminar certificados caducados**.

   Los certificados de cifrado caducados utilizados para S/MIME deben conservarse en el dispositivo para que los usuarios puedan leer los mensajes cifrados antes de la caducidad del certificado de cifrado.
8. Si desea que el dispositivo elimine certificados duplicados, seleccione **Eliminar certificado duplicado**. El dispositivo elimina el certificado que tiene la fecha de inicio más inmediata.
9. Haga clic en **Agregar**.

Después de terminar:

- Permita que las aplicaciones de BlackBerry Dynamics usen certificados.
- Asigne el perfil a las cuentas de usuario y los grupos de usuarios.

Envío de certificados de cliente a dispositivos y aplicaciones mediante SCEP

Puede utilizar perfiles SCEP para especificar cómo los dispositivos y las aplicaciones de BlackBerry Dynamics obtienen certificados de cliente de la CA de la empresa a través de un servicio SCEP. SCEP es un protocolo IETF que simplifica el proceso de inscripción de certificados de cliente en un gran número de dispositivos o aplicaciones sin necesidad de ninguna introducción de datos o aprobación por parte del administrador para emitir cada certificado. Los dispositivos y las aplicaciones de BlackBerry Dynamics pueden usar SCEP para solicitar y obtener certificados de cliente de una CA compatible con SCEP que utilice la empresa.

La CA que utilice debe admitir contraseñas de comprobación. La CA utiliza contraseñas de comprobación para verificar que el dispositivo o la aplicación estén autorizados a enviar una solicitud de certificado.

Para utilizar SCEP en un entorno BlackBerry UEM Cloud es necesario instalar la versión más reciente de BlackBerry Connectivity Node para que BlackBerry UEM Cloud pueda acceder al directorio de la empresa.

Si su empresa utiliza una CA de Entrust o CA de OpenTrust, los perfiles de SCEP no son compatibles para los dispositivos con Windows 10.

Crear un perfil SCEP

La configuración de perfil necesaria depende de la configuración del servicio SCEP en el entorno de su empresa y varía en función de si el certificado lo utiliza una aplicación de BlackBerry Dynamics o un tipo de dispositivo especificado.

Puede utilizar una variable en cualquier campo de texto para hacer referencia a un valor en lugar de especificar el valor real.

Nota: Si desea utilizar un perfil de SCEP para distribuir certificados de cliente de OpenTrust a los dispositivos, debe realizar una revisión de su software de OpenTrust. Para obtener más información, póngase en contacto con su representante de soporte de OpenTrust y consulte el caso de soporte SUPPORT-798.

1. En la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Certificados > SCEP**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil. Cada perfil de certificado debe tener un nombre único.
5. En la lista desplegable **Conexión con la autoridad de certificación**, lleve a cabo una de las acciones siguientes:
   - Para utilizar una conexión de Entrust que haya configurado, haga clic en la conexión correspondiente. En la lista desplegable **Perfil**, haga clic en un perfil. Especifique los valores para el perfil.
   - Para utilizar una conexión de OpenTrust que haya configurado, haga clic en la conexión correspondiente. En la lista desplegable **Perfil**, haga clic en un perfil. Especifique los valores para el perfil.
     - Las siguientes opciones del perfil de SCEP no se aplican a los certificados de cliente de OpenTrust: Uso de la clave, Uso extendido de la clave, Asunto y SAN.
   - Para utilizar otra CA, haga clic en **Genérico**. En la lista desplegable **Tipo de desafío SCEP**, seleccione **Estático** o **Dinámico** y especifique los ajustes necesarios para el tipo de desafío.

     Nota: Para los dispositivos con Windows, únicamente se admiten contraseñas estáticas.
6. En el campo **URL**, escriba la URL para el servicio SCEP. La URL debe incluir el protocolo, FQDN, el número de puerto y la ruta SCEP.
7. En el campo **Nombre de la instancia**, escriba el nombre de la instancia para la CA.
8. Opcionalmente, desactive la casilla de verificación para cualquier tipo de dispositivo para el que no desee configurar el perfil.
9. Realice las acciones siguientes:
   a) Haga clic en la pestaña de un tipo de dispositivo.
   b) Configure los valores adecuados para cada configuración del perfil para que coincida con la configuración del servicio SCEP del entorno de la empresa.
10. Repita el paso 8 para cada tipo de dispositivo en la empresa.
11. Haga clic en **Agregar**.

Después de terminar: Si los dispositivos utilizan el certificado de cliente para autenticarse en una red de Wi-Fi de trabajo, una VPN de trabajo o un servidor de correo de trabajo, debe asociar el perfil de SCEP con Wi-Fi, una VPN, o un perfil de correo electrónico.

Ajustes del perfil SCEP

Los perfiles SCEP son compatibles con los siguientes tipos de dispositivos:

- iOS
- macOS
- Android
- Windows 10

Común: ajustes del perfil SCEP

Común: configuración del perfil SCEP	Descripción
Conexión con la autoridad de certificación	Esta configuración especifica si la CA es Entrust, OpenTrust u otra CA. Si ha configurado una o más conexiones al software Entrust o OpenTrust de la empresa, puede seleccionar una de las conexiones en la lista desplegable. Seleccione Genérico si está usando cualquier otra CA. Si selecciona una conexión Entrust o OpenTrust, a continuación debe seleccionar el perfil de PKI adecuado y especificar los valores necesarios. Los perfiles disponibles varían en función de lo que el administrador de Entrust o OpenTrust haya configurado en el software de PKI. El valor predeterminado es Genérico.
URL	Este ajuste especifica la URL del servicio SCEP. La URL debe incluir el protocolo, el FQDN, el número de puerto y la ruta SCEP (la ruta CGI que se define en la especificación SCEP). Debe establecer un valor la configuración para activar un dispositivo correctamente. Las URL HTTPS de SCEP son compatibles con los dispositivos iOS.
Nombre de la instancia	Este ajuste especifica el nombre de la instancia de la autoridad de certificación. El valor puede ser cualquier cadena que sea entendida por el servicio SCEP. Por ejemplo, podría tratarse de un nombre de dominio como example.org. Si una CA tiene varios certificados de CA, este campo puede utilizarse para distinguir cuál se necesita.
Comprobar cadena de confianza de conexión al servidor SCEP	Esta configuración especifica si BlackBerry UEM verifica que la raíz CA del servidor SCEP se ha almacenado en el almacén de certificados BlackBerry UEM para permitir que BlackBerry UEM confíe en el servidor SCEP cuando se prueben las conexiones, se recuperen contraseñas de comprobación y actúe como proxy para las solicitudes de SCEP de los dispositivos.

Común: configuración del perfil SCEP	Descripción
Tipo de desafío SCEP	En la configuración se especifica si la contraseña de comprobación SCEP se genera dinámicamente o como una contraseña estática. Si la configuración se establece en "Estático", todos los dispositivos utilizarán la misma contraseña de comprobación. Si la configuración se establece en "Dinámico", cada dispositivo recibirá una contraseña de comprobación exclusiva. Valores posibles: • Estático • Dinámico El valor predeterminado es Dinámico. Para los dispositivos con Windows, únicamente se admiten contraseñas "Estáticas".
URL de generación de contraseñas de comprobación	En la configuración se especifica la URL que el dispositivo utiliza para obtener una contraseña de comprobación generada dinámicamente desde el servicio SCEP. La URL debe incluir el protocolo, el dominio, el puerto y la ruta SCEP (la ruta CGI que se define en la especificación SCEP). Esta configuración es válida únicamente si la opción "Tipo de desafío SCEP" se establece en "Dinámico".
Tipo de autenticación	En la configuración se especifica el tipo de autenticación que los dispositivos utilizan para conectarse al servicio SCEP y obtener una contraseña de comprobación. Esta configuración es válida únicamente si la opción "Tipo de desafío SCEP" se establece en "Dinámico". Valores posibles: • Básico • NTLM El valor predeterminado es Básico.
Dominio	En la configuración se especifica el dominio utilizado para la autenticación NTLM cuando los dispositivos se conectan al servicio SCEP para obtener una contraseña de comprobación. Esta configuración es válida únicamente si la opción "Tipo de autenticación" se establece en "NTLM".
Nombre de usuario	La contraseña especifica el nombre de usuario requerido para obtener una contraseña de comprobación desde el servicio SCEP. Esta configuración es válida únicamente si la opción "Tipo de desafío SCEP" se establece en "Dinámico".

Común: configuración del perfil SCEP	Descripción
Contraseña	La contraseña especifica la contraseña requerida para obtener la contraseña de comprobación desde el servicio SCEP. Esta configuración es válida únicamente si la opción "Tipo de desafío SCEP" se establece en "Dinámico".
Contraseña de comprobación	Esta configuración especifica la contraseña de comprobación que un dispositivo utiliza para la inscripción de certificados. Esta configuración es válida únicamente si la opción "Tipo de desafío SCEP" se establece en "Estático".

iOS: Ajustes del perfil SCEP

iOS: Ajustes del perfil SCEP	Descripción
Usar BlackBerry UEM como proxy para solicitudes SCEP	Esta configuración especifica si todas las solicitudes SCEP de los dispositivos se envían a través de BlackBerry UEM. Si la CA está detrás del firewall, la configuración permitirá inscribir certificados de cliente en los dispositivos sin exponer la CA fuera del firewall.
Utilice BlackBerry Connectivity Node para la conectividad CA	Esta configuración especifica si las solicitudes SCEP deben enrutarse a través de BlackBerry Connectivity Node. Este ajuste solo se muestra en BlackBerry UEM Cloud.
Asunto	Esta configuración especifica el asunto del certificado, si es necesario para la configuración SCEP de la empresa. Escriba el asunto en el formato "/CN=<*common_name*>/O=<*domain_name*>". Si el perfil es para varios usuarios, puede utilizar una variable, por ejemplo: %UserDistinguishedName%.
Reintentos	En la configuración se especifica cuántas veces debe volver a intentarse la conexión al servicio SCEP si el intento de conexión falla. Los valores posibles son de 1 a 999. El valor predeterminado es "3".
Intervalo entre reintentos	En la configuración se especifica el tiempo en segundos que hay que esperar antes de intentar conectarse al servicio SCEP. Los valores posibles son de 1 a 999. El valor predeterminado es "10" segundos.

iOS: Ajustes del perfil SCEP	Descripción
Tamaño de clave	Esta configuración especifica el tamaño de clave para el certificado. Valores posibles: • 1024 • 2048 • 4096 El valor predeterminado es 1024.
Huella dactilar	Esta configuración especifica la huella digital para inscribir un certificado SCEP. Si la CA utiliza HTTP en lugar de HTTPS, los dispositivos utilizan la huella digital para confirmar la identidad de la CA durante el proceso de inscripción. La huella dactilar no puede contener espacios.
Tipo de SAN	Esta configuración especifica el tipo de nombre alternativo del asunto del certificado, si es necesario. Valores posibles: • Ninguno • Nombre de RFC822 • Nombre de DNS • Identificador de recursos uniforme El valor predeterminado es "Ninguno".
Valor de SAN	Esta configuración especifica la representación alternativa del asunto del certificado. El valor debe ser una dirección de correo, el nombre DNS del servidor CA, la URL completa del servidor. El ajuste "Tipo de SAN" determina el valor adecuado que se debe especificar. Si se establece en "Nombre de RFC822" el valor debe ser una dirección de correo válida. Si se establece en "URI", el valor debe ser una URL válida que incluya el protocolo y la dirección IP o FQDN. Si se establece en "Nombre principal de NT", el valor debe ser un nombre principal válido. Si se establece en "Nombre de DNS", el valor debe ser un FQDN válido.
Nombre principal de NT	Esta configuración especifica el nombre principal de NT para la generación del certificado. Esta configuración es válida únicamente si la opción "Tipo de SAN" se establece en un valor distinto de "Ninguno".
Caducidad del perfil	Especifique el número de días después de la emisión del certificado en el que el dispositivo solicita un nuevo certificado de la CA. El valor debe ser inferior al periodo de validez del certificado definido por la CA. El valor máximo es 1825 días.

macOS: Ajustes del perfil SCEP

macOS aplica perfiles a las cuentas de usuario o los dispositivos. Puede configurar perfiles SCEP para aplicarlos a uno u otro.

macOS: Ajustes del perfil SCEP	Descripción
Usar BlackBerry UEM como proxy para solicitudes SCEP	Esta configuración especifica si todas las solicitudes SCEP de los dispositivos se envían a través de BlackBerry UEM. Si la CA está detrás del firewall, la configuración permitirá inscribir certificados de cliente en los dispositivos sin exponer la CA fuera del firewall.
Utilice BlackBerry Connectivity Node para la conectividad CA	Esta configuración especifica si las solicitudes SCEP deben enrutarse a través de BlackBerry Connectivity Node. Este ajuste solo se muestra en BlackBerry UEM Cloud.
Aplicar perfil a	En la configuración se especifica si el perfil SCEP se aplica a la cuenta de usuario o al dispositivo. Valores posibles: • Usuario • Dispositivo
Asunto	Esta configuración especifica el asunto del certificado, si es necesario para la configuración SCEP de la empresa. Escriba el asunto en el formato "/CN=<*common_name*>/O=<*domain_name*>". Si el perfil es para varios usuarios, puede utilizar una variable, por ejemplo: %UserDistinguishedName%.
Reintentos	En la configuración se especifica cuántas veces debe volver a intentarse la conexión al servicio SCEP si el intento de conexión falla. Los valores posibles son de 1 a 999. El valor predeterminado es "3".
Intervalo entre reintentos	En la configuración se especifica el tiempo en segundos que hay que esperar antes de intentar conectarse al servicio SCEP. Los valores posibles son de 1 a 999. El valor predeterminado es "10" segundos.
Tamaño de clave	Esta configuración especifica el tamaño de clave para el certificado. Valores posibles: • 1024 • 2048 El valor predeterminado es "1024".
Huella dactilar	Esta configuración especifica la huella digital para inscribir un certificado SCEP. Si la CA utiliza HTTP en lugar de HTTPS, los dispositivos utilizan la huella digital para confirmar la identidad de la CA durante el proceso de inscripción. La huella dactilar no puede contener espacios.

macOS: Ajustes del perfil SCEP	Descripción
Tipo de SAN	Esta configuración especifica el tipo de nombre alternativo del asunto del certificado, si es necesario. Valores posibles: • Ninguno • Nombre de RFC822 • Nombre de DNS • Identificador de recursos uniforme El valor predeterminado es "Ninguno".
Valor de SAN	Esta configuración especifica la representación alternativa del asunto del certificado. El valor debe ser una dirección de correo, el nombre DNS del servidor CA, la URL completa del servidor. El ajuste "Tipo de SAN" determina el valor adecuado que se debe especificar. Si se establece en "Nombre de RFC822" el valor debe ser una dirección de correo válida. Si se establece en "URI", el valor debe ser una URL válida que incluya el protocolo y la dirección IP o FQDN. Si se establece en "Nombre principal de NT", el valor debe ser un nombre principal válido. Si se establece en "Nombre de DNS", el valor debe ser un FQDN válido.
Nombre principal de NT	Esta configuración especifica el nombre principal de NT para la generación del certificado. Esta configuración es válida únicamente si la opción "Tipo de SAN" se establece en un valor distinto de "Ninguno".

Android: configuración del perfil de SCEP

Para ver un ejemplo de un perfil SCEP para dispositivos con Android, visite support.blackberry.com/community/ para leer el artículo 38248.

Android: configuración del perfil SCEP	Descripción
Usar BlackBerry UEM como proxy para solicitudes SCEP	En la configuración se especifica si todas las solicitudes SCEP desde los dispositivos se envían a través de BlackBerry UEM. Si la CA está detrás del firewall, la configuración permitirá inscribir certificados de cliente en los dispositivos sin exponer la CA fuera del firewall.
Ocultar certificado en dispositivos con Android Enterprise	Esta configuración especifica si el certificado es visible para los usuarios con Android 9.0 y versiones de Android Enterprise posteriores. Si el certificado está oculto, los usuarios no pueden seleccionarlo para utilizarlo con fines adicionales.
Utilice BlackBerry Connectivity Node para la conectividad CA	Esta configuración especifica si las solicitudes SCEP deben enrutarse a través de BlackBerry Connectivity Node. Esta configuración solo se muestra en BlackBerry UEM Cloud.

Android: configuración del perfil SCEP	Descripción
Algoritmo de cifrado	Esta configuración especifica el algoritmo de cifrado que los dispositivos con Android utilizan para la solicitud de inscripción de certificados. Valores posibles: • Ninguno • Triple DES • AES (128 bits) • AES (196 bits) • AES (256 bits) El valor predeterminado es "Triple DES".
Función hash	Esta configuración especifica la función hash que los dispositivos con Android utilizan para la solicitud de inscripción de certificados. Valores posibles: • Ninguno • SHA-1 • SHA-224 • SHA-256 • SHA-384 • SHA-512 El valor predeterminado es "SHA-1".
Huella digital de certificado	Esta configuración especifica el hash de cifrado hexadecimal del certificado raíz para la autoridad de certificación. Puede utilizar los siguientes algoritmos para especificar la huella digital: SHA-1, SHA-224, SHA-256, SHA-384 y SHA-512. Debe establecer un valor para esta configuración para que se activen correctamente dispositivos con Android Enterprise o Samsung Knox.
Renovación automática	Esta configuración especifica cuántos días antes de que caduque el certificado debe realizarse la renovación automática. Los valores posibles son de 1 a 365. El valor predeterminado es "30".
Android Enterprise/Samsung KNOX	
Asunto	Esta configuración especifica el asunto del certificado, si es necesario para la configuración SCEP de la empresa. Escriba el asunto en el formato "/CN=<*common_name*>/O=<*domain_name*>". Si el perfil es para varios usuarios, puede utilizar una variable, por ejemplo: %UserDistinguishedName%.

Android: configuración del perfil SCEP	Descripción
Tipo de SAN	Esta configuración especifica el tipo de nombre alternativo del asunto del certificado, si es necesario. Valores posibles: • Nombre de RFC 822 • Identificador de recursos uniforme • Nombre principal de NT • Nombre de DNS El valor predeterminado es "Nombre de RFC 822".
Valor de SAN	Esta configuración especifica la representación alternativa del asunto del certificado. El valor debe ser una dirección de correo, el nombre DNS del servidor CA, la URL completa del servidor o el nombre principal. El ajuste "Tipo de SAN" determina el valor adecuado que se debe especificar. Si se establece en "Nombre de RFC822" el valor debe ser una dirección de correo válida. Si se establece en "URI", el valor debe ser una URL válida que incluya el protocolo y la dirección IP o FQDN. Si se establece en "Nombre principal de NT", el valor debe ser un nombre principal válido. Si se establece en "Nombre de DNS", el valor debe ser un FQDN válido.
Algoritmo de clave	Esta configuración especifica el algoritmo que los dispositivos con Android Enterprise y Samsung Knox deben utilizar para generar el par de claves del cliente. Debe seleccionar un algoritmo que sea compatible con su CA. Valores posibles: • Ninguno • RSA • ECC El valor predeterminado es "RSA".
Intensidad de RSA	Esta configuración especifica la intensidad de RSA que los dispositivos con Android Enterprise y Samsung Knox deben utilizar para generar el par de claves del cliente. Debe introducir una intensidad de la clave que sea compatible con su CA. Esta configuración solo es válida si la opción "Algoritmo de clave" se establece en "RSA". Valores posibles: • 1024 • 2048 • 4096 • 8192 • 16384 El valor predeterminado es "1024".

Android: configuración del perfil SCEP	Descripción
Uso de la clave	Esta configuración especifica las operaciones criptográficas que se pueden realizar con la clave pública que está incluida en el certificado. Selecciones posibles: • Firma digital • Sin rechazo • Cifrado de clave • Cifrado de datos • Acuerdo de clave • Firma del certificado de clave • Firma de CRL • Solo cifrado • Solo descifrado Las selecciones predeterminadas son "Firma digital", "Cifrado de clave" y "Acuerdo de clave".
Uso extendido de la clave	Esta configuración especifica la finalidad de la clave que está incluida en el certificado. Selecciones posibles: • Autenticación de servidor • Autenticación de cliente • Firma de código • Protección de correo • Marca de hora • Firma de OCSP • Cliente de shell seguro • Servidor de shell seguro La selección predeterminada es "Autenticación de cliente".

Windows 10: configuración del perfil de SCEP

Windows 10: configuración del perfil SCEP	Descripción
Almacén de certificados del usuario	Esta configuración especifica si el certificado debe almacenarse en la ubicación de certificados del usuario en el dispositivo.
Asunto	Esta configuración especifica el asunto del certificado, si es necesario para la configuración SCEP de la empresa. Escriba el asunto en el formato "/CN=<*common_name*>/O=<*domain_name*>". Si el perfil es para varios usuarios, puede utilizar una variable, por ejemplo: %UserDistinguishedName%.

Windows 10: configuración del perfil SCEP	Descripción
Tipo de SAN	Esta configuración especifica el tipo de nombre alternativo del asunto del certificado, si es necesario. Valores posibles: • Ninguno • Nombre de RFC 822 • Nombre de DNS • Identificador de recursos uniforme El valor predeterminado es "Ninguno".
Valor de SAN	Esta configuración especifica la representación alternativa del asunto del certificado. El valor debe ser una dirección de correo, el nombre DNS del servidor CA, la URL completa del servidor. El valor apropiado para este ajuste dependerá del valor seleccionado para el ajuste "Tipo de SAN".
Reintentos	En la configuración se especifica cuántas veces debe volver a intentarse la conexión al servicio SCEP si el intento de conexión falla. Los valores posibles son de 1 a 999. El valor predeterminado es "3".
Intervalo entre reintentos	En la configuración se especifica el tiempo en segundos que hay que esperar antes de intentar conectarse al servicio SCEP. Los valores posibles son de 1 a 999. El valor predeterminado es "10" segundos.
Tamaño de clave	Esta configuración especifica el tamaño de clave para el certificado. Valores posibles: • 1024 • 2048 • 4096 • 8192 • 16384 El valor predeterminado es "1024".

Windows 10: configuración del perfil SCEP	Descripción
Uso de la clave	Esta configuración especifica las operaciones criptográficas que se pueden realizar con la clave pública que está incluida en el certificado. • Firma digital • Sin rechazo • Cifrado de clave • Cifrado de datos • Acuerdo de clave • Firma del certificado de clave • Firma de CRL • Solo cifrado Las selecciones predeterminadas son "Firma del certificado de clave" y "Solo cifrado".
Uso extendido de la clave	Esta configuración especifica la finalidad de la clave que está incluida en el certificado. • Autenticación de servidor • Autenticación de cliente • Firma de código • Protección de correo • Marca de hora • Firma de OCSP • Cliente de shell seguro • Servidor de shell seguro La selección predeterminada es "Autenticación de cliente".
Almacenamiento de claves de SCEP	Esta configuración especifica la ubicación de almacenamiento de la clave privada. Valores posibles: • TPM • TPM si es compatible • KSP El valor predeterminado es "KSP".
Función hash	Esta configuración especifica la función hash que un dispositivo con Windows 10 utiliza para la solicitud de inscripción de certificados. Valores posibles: • SHA-1 • SHA-224 • SHA-256 • SHA-384 • SHA-512 El valor predeterminado es "SHA-1".

Windows 10: configuración del perfil SCEP	Descripción
Huella digital de certificado	Esta configuración especifica el hash de cifrado hexadecimal del certificado raíz para la autoridad de certificación. Puede utilizar los siguientes algoritmos para especificar la huella digital: SHA-1, SHA-224, SHA-256, SHA-384 y SHA-512.
Renovación automática	Esta configuración especifica cuántos días antes de que caduque el certificado debe realizarse la renovación automática. Los valores posibles son de 1 a 365. El valor predeterminado es "30".

BlackBerry Dynamics: configuración del perfil de SCEP

Esta configuración se aplica a los certificados SCEP utilizados con aplicaciones de BlackBerry Dynamics en dispositivos con iOS y Android.

BlackBerry Dynamics: configuración del perfil SCEP	Descripción
Asunto	Esta configuración especifica el asunto del certificado, si es necesario para la configuración SCEP de la empresa. Escriba el asunto en el formato "/CN=<*common_name*>/O=<*domain_name*>". Si el perfil es para varios usuarios, puede utilizar una variable, por ejemplo: %UserDistinguishedName%.
Tipo de SAN	Esta configuración especifica el tipo de nombre alternativo del asunto del certificado, si es necesario. Valores posibles: • Nombre de RFC 822 • Identificador de recursos uniforme • Nombre principal de NT • Nombre de DNS El valor predeterminado es "Nombre de RFC 822".
Valor de SAN	Esta configuración especifica la representación alternativa del asunto del certificado. El valor debe ser una dirección de correo, el nombre DNS del servidor CA, la URL completa del servidor o el nombre principal. El ajuste "Tipo de SAN" determina el valor adecuado que se debe especificar. Si se establece en "Nombre de RFC822" el valor debe ser una dirección de correo válida. Si se establece en "URI", el valor debe ser una URL válida que incluya el protocolo y la dirección IP o FQDN. Si se establece en "Nombre principal de NT", el valor debe ser un nombre principal válido. Si se establece en "Nombre de DNS", el valor debe ser un FQDN válido.

BlackBerry Dynamics: configuración del perfil SCEP	Descripción
Algoritmo de clave	Esta configuración especifica el algoritmo que un dispositivo debe utilizar para generar el par de claves del cliente. Debe seleccionar un algoritmo que sea compatible con su CA. Valores posibles: • RSA
Intensidad de RSA	Esta configuración especifica la intensidad de RSA utilizada para generar el par de claves del cliente. Debe introducir una intensidad de la clave que sea compatible con su CA. Esta configuración solo es válida si la opción "Algoritmo de clave" se establece en "RSA". Valores posibles: • 2048 • 4096 El valor predeterminado es "2048".
Algoritmo de cifrado	Esta configuración especifica el algoritmo de cifrado utilizado para la solicitud de inscripción de certificados. Valores posibles: • Triple DES • AES (128 bits) • AES (196 bits) • AES (256 bits) El valor predeterminado es "Triple DES".
Función hash	Esta configuración especifica la función hash utilizada para la solicitud de inscripción de certificados. Valores posibles: • SHA-256 • SHA-384 • SHA-512 El valor predeterminado es "SHA-256".
Huella digital de certificado	Esta configuración especifica el hash de cifrado hexadecimal del certificado raíz para la autoridad de certificación. Puede utilizar uno de los siguientes algoritmos para especificar la huella digital: SHA-1, SHA-224, SHA-256, SHA-384 y SHA-512. MD5 solo es compatible si "Activar FIPS" no está seleccionado en el perfil BlackBerry Dynamics.

BlackBerry Dynamics: configuración del perfil SCEP	Descripción
Renovación automática	Esta configuración especifica cuántos días antes de que caduque el certificado debe realizarse la renovación automática. Los valores posibles son de 1 a 365. El valor predeterminado es "30".
Uso de la clave	Esta configuración especifica las operaciones criptográficas que se pueden realizar con la clave pública que está incluida en el certificado. Selecciones posibles: • Firma digital • Sin rechazo • Cifrado de clave • Cifrado de datos • Acuerdo de clave • Firma del certificado de clave • Firma de CRL • Solo cifrado • Solo descifrado Las selecciones predeterminadas son "Firma digital", "Cifrado de clave" y "Acuerdo de clave".
Uso extendido de la clave	Esta configuración especifica la finalidad de la clave que está incluida en el certificado. Selecciones posibles: • Autenticación de servidor • Autenticación de cliente • Firma de código • Protección de correo • Marca de hora • Firma de OCSP • Cliente de shell seguro • Servidor de shell seguro La selección predeterminada es "Autenticación de cliente".
Restricciones de aplicaciones	En la configuración se especifican las aplicaciones de BlackBerry Dynamics que pueden utilizar el certificado. Valores posibles: • Permitir que todas las aplicaciones utilicen certificados • Permitir que aplicaciones específicas utilicen certificados La selección predeterminada es "Permitir que todas las aplicaciones utilicen certificados".

BlackBerry Dynamics: configuración del perfil SCEP	Descripción
Aplicaciones con permiso para utilizar SCEP	En la configuración se especifican las aplicaciones de BlackBerry Dynamics que pueden utilizar certificados SCEP. Esta configuración es válida únicamente si la opción "Restricciones de aplicación" se establece en "Permitir que las aplicaciones especificadas utilicen certificados".
Eliminar certificados caducados	Esta configuración especifica si el dispositivo debe borrar los certificados caducados.
Eliminar certificados duplicados	Esta configuración especifica si el dispositivo debe borrar los certificados duplicados. El dispositivo elimina el certificado que tiene la fecha de inicio más inmediata.

Envío del mismo certificado de cliente a varios dispositivos

Puede utilizar perfiles de certificados compartidos para enviar certificados de cliente a los dispositivos iOS, macOS y Android.

Los perfiles de certificado compartido envían el mismo par de claves a cada usuario al que se le ha asignado el perfil. Debe utilizar perfiles de certificado compartido solo si desea permitir a más de un usuario compartir un certificado de cliente.

macOS aplica perfiles a las cuentas de usuario o los dispositivos. Puede configurar un perfil de certificado compartido para aplicarlo a una u otra opción.

Creación de un perfil de certificado compartido

Antes de empezar: Debe obtener el archivo del certificado de cliente que desea enviar a los dispositivos. El archivo del certificado debe tener una extensión de nombre de archivo .pfx o p12.

1. En la barra de menú, haga clic en **Políticas y perfiles**.
2. Haga clic en **Certificados > Certificado compartido**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil. Cada perfil de certificado debe tener un nombre único. Algunos nombres (por ejemplo, ca_1) están reservados.
5. En el campo **Contraseña**, escriba una contraseña para el perfil de certificado compartido.
6. En el campo **Archivo de certificado**, haga clic en **Examinar** para ubicar el archivo de certificado.
7. Si está administrando dispositivos Android Enterprise y desea evitar que los usuarios seleccionen el certificado para utilizarlo con otros fines, en la pestaña **Android** seleccione **Ocultar certificado en dispositivos Android Enterprise**. Esta opción se aplica únicamente a dispositivos con Android 9.0 o versiones posteriores.
8. Si está gestionando dispositivos macOS, en la pestaña **macOS**, en la lista desplegable **Aplicar perfil a**, seleccione **Usuario** o **Dispositivo**.
9. Haga clic en **Agregar**.

Especificar el certificado utilizado por una aplicación

Para los dispositivos Android, puede utilizar un perfil de asignación de certificados para especificar los certificados de cliente que utilizan las aplicaciones. El perfil de asignación de certificados no es compatible con las aplicaciones de BlackBerry Dynamics.

Los perfiles de asignación de certificados le permiten especificar los certificados que utilizan las aplicaciones de Android. Puede disponer que una aplicación utilice un certificado enviado al dispositivo mediante SCEP, credenciales de usuario o un perfil de certificado compartido. Puede utilizar un certificado con una o varias de las aplicaciones gestionadas, o todas. También puede especificar si una aplicación utiliza un certificado cada vez que se le solicita o únicamente para las conexiones a un URI determinado.

Se pueden especificar varias asignaciones de certificados en un mismo perfil. Solo se puede asignar un perfil de asignación de certificados a un usuario.

Creación de un perfil de asignación de certificados

Antes de empezar: Cree los perfiles SCEP, de credenciales de usuario o de certificado compartido necesarios para enviar certificados a dispositivos y asigne los perfiles a usuarios o grupos.

1. En la barra de menú, haga clic en **Políticas y perfiles**.
2. Haga clic en Certificados > Asignación de certificados.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil. Cada perfil de certificado debe tener un nombre único.
5. En la tabla de asignación, haga clic en +.
6. En **URI de destino**, seleccione una de las siguientes opciones:
   - Seleccione **Ninguno** si la aplicación no utiliza el certificado para autenticar una conexión con un recurso.
   - Seleccione **Cualquiera** si la aplicación puede utilizar el certificado para autenticar una conexión con cualquier recurso.
   - Seleccione **Host especificado: puerto** y escriba el host y el puerto si la aplicación puede utilizar el certificado para autenticar una conexión con un recurso específico.
7. En **Certificado de la aplicación**, lleve a cabo una de las acciones siguientes:
   - Para especificar que la aplicación debe utilizar un certificado enviado al dispositivo por otro perfil, seleccione **Certificado seleccionado** y seleccione el nombre del perfil en la lista desplegable.
   - Para especificar que la aplicación debe utilizar un certificado enviado al dispositivo por un tercero, seleccione **Alias de certificado** y escriba el alias del certificado. Si no conoce el alias, consulte la documentación o el administrador del proveedor del certificado.
   - Para especificar que la aplicación debe utilizar un certificado enviado al dispositivo por otro perfil, seleccione **Certificado seleccionado** y seleccione el nombre del perfil en la lista desplegable.
8. En **Aplicaciones con permiso para el URI de destino**, lleve a cabo una de las siguientes acciones:
   - Para permitir que cualquier aplicación gestionada pueda solicitar el certificado especificado, seleccione **Cualquier aplicación del espacio de trabajo**.
   - Para permitir que únicamente las aplicaciones especificadas soliciten el certificado, seleccione **Aplicaciones especificadas** y haga clic en + para especificar una o varias aplicaciones.
9. Si fuera necesario, repita los pasos de 5 a 8 para agregar asignaciones adicionales al perfil.
10. Haga clic en **Agregar**.

Después de terminar:

- Asigne el perfil a las cuentas de usuario y los grupos de usuarios.

- Si fuera necesario, clasifique los perfiles.

Administración de certificados de cliente para cuentas de usuarios

Puede agregar certificados de cliente directamente a cuentas de usuarios individuales o a un perfil de credenciales de usuario asignado a la cuenta de este. Agregar certificados directamente a una cuenta de usuario es compatible con los dispositivos activados con BlackBerry Dynamics o con otros dispositivos con iOS y Android administrados. La carga de certificados en perfiles de credenciales de usuario es compatible con dispositivos con iOS y dispositivos con Android Enterprise.

Para permitir que los usuarios carguen certificados que puedan utilizar para conectarse a su red de Wi-Fi de trabajo, red VPN de trabajo y servidor de correo del trabajo, utilice un perfil de credenciales de usuario que pueda asociarse a un Wi-Fi, una VPN o a un perfil de correo electrónico.

Si tiene un entorno local y carga certificados para aplicaciones de BlackBerry Dynamics en cuentas de usuario, debe configurar un periodo de validez de certificados de cliente. Cuando el periodo de validez finaliza, los certificados se eliminan del servidor.

Adición de un certificado de cliente a una cuenta de usuario

Puede agregar un certificado de cliente a una cuenta de usuario individual y enviar el certificado a dispositivos con BlackBerry Dynamics u otros dispositivos gestionados iOS y Android.

Agregue certificados de cliente a cuentas de usuario cuando los dispositivos de usuarios necesiten certificados para S/MIME o autenticación de cliente y el certificado no se pueda enviar a los dispositivos a través de un perfil de credenciales de usuario o perfil SCEP.

El certificado de cliente debe tener una extensión de nombre de archivo .pfx o p12. Puede enviar más de un certificado de cliente a los dispositivos.

También puede utilizar los perfiles de credenciales de usuario para cargar certificados para usuarios individuales. Los perfiles de credenciales de usuario se pueden asociar a un perfil de Wi-Fi, VPN o correo.

1. En la barra de menú, 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 una cuenta de usuario.
4. En la sección **Política de TI y perfiles**, haga clic en +.
5. Haga clic en **Certificado de usuario**.
6. Escriba una descripción para el certificado.
7. En la sección **Aplicar certificado a**, seleccione una de las opciones siguientes:
   - **Otros dispositivos gestionados**: seleccione esta opción para enviar el certificado a dispositivos iOS y Android para todos los usos admitidos excepto para aplicaciones de BlackBerry Dynamics.
   - **Dispositivos con BlackBerry Dynamics**: seleccione esta opción para enviar el certificado a dispositivos para utilizarlo con aplicaciones de BlackBerry Dynamics.
8. En el campo **Archivo de certificado**, haga clic en **Examinar** para ubicar el archivo de certificado.
9. Si ha seleccionado **Otros dispositivos administrados**, en el campo **Contraseña**, escriba una contraseña para el certificado. Para dispositivos iOS, se requiere una contraseña. Para dispositivos Android, no es necesario proporcionar una contraseña en BlackBerry UEM si el dispositivo dispone de la última versión de BlackBerry UEM Client. Si no establece una contraseña, el usuario debe introducir la contraseña del dispositivo.
10. Haga clic en **Agregar**.
    El certificado se incluye en la tabla **Certificados de usuario** de la página de resumen de usuario.

Después de terminar:

- Para dispositivos BlackBerry Dynamics, configure el periodo de tiempo en que los certificados cargados permanecen en el servidor de BlackBerry UEM antes de que se eliminen automáticamente de este. La configuración predeterminada es 24 horas.

Cambie un certificado de cliente por una cuenta de usuario

1. En la barra de menú, 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 una cuenta de usuario.
4. En la sección **Política de TI y perfiles**, haga clic en el certificado de usuario que desea cambiar.
5. Haga clic en .
6. Realice los cambios necesarios. No puede cambiar los dispositivos a los que se aplica el certificado.
7. Haga clic en **Guardar**.

Después de terminar: Si cambia un certificado de usuario de BlackBerry Dynamics que usted o un usuario han eliminado de un dispositivo, el certificado se volverá a enviar al dispositivo.

Renovación o eliminación de un certificado de BlackBerry Dynamics para una cuenta de usuario

Puede enviar un comando al dispositivo de un usuario para solicitar la renovación del certificado de la entidad de certificación. También puede eliminar un certificado de BlackBerry Dynamics del dispositivo de un usuario. Si elimina un certificado, el conector de PKI de BlackBerry Dynamics envía una notificación a la entidad de certificación de que el certificado ya no está en uso, aunque el certificado no se revoca automáticamente.

1. En la barra de menú, 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 una cuenta de usuario.
4. En la sección **Certificados de usuario**, realice una de las siguientes acciones:
   - Haga clic en para solicitar la renovación del certificado de la CA.
   - Haga clic en para eliminar el certificado de los dispositivos del usuario.

   Nota: Para eliminar una credencial inteligente de Entrust de un dispositivo, el usuario también debe desactivar la credencial inteligente en BlackBerry UEM Client.

Adición de un certificado de cliente a un perfil de credenciales de usuario

Puede cargar certificados para usuarios individuales a un perfil de credenciales de usuario. Los usuarios también pueden cargar su certificado al perfil de credenciales de usuario mediante BlackBerry UEM Self-Service. La carga de certificados en perfiles de credenciales de usuario es compatible con dispositivos con iOS y para dispositivos con Android Enterprise.

El certificado de cliente debe tener una extensión de nombre de archivo .pfx o p12. Si se carga un certificado nuevo al perfil de credenciales de usuario, se sustituye el certificado existente en los dispositivos de usuario.

Antes de empezar:

- Cree un perfil de credenciales de usuario para cargar manualmente los certificados.
- Asigne el perfil de credenciales de usuario a los usuarios.

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 una cuenta de usuario.
4. En la sección **Política de TI y perfiles**, junto al perfil de credenciales de usuario, haga clic en **Agregar certificado**.
5. Haga clic en **Examinar** para buscar el archivo de certificado.
6. Introduzca la contraseña del certificado. Para dispositivos iOS, se requiere la contraseña. Para dispositivos Android, no es necesario proporcionar la contraseña en BlackBerry UEM si el dispositivo dispone de la última versión de BlackBerry UEM Client. Si no especifica la contraseña, el usuario debe introducir la contraseña del dispositivo.
7. Haga clic en **Agregar**.

Cambie un certificado de cliente por un perfil de credenciales de usuario

Puede cambiar el certificado que se ha añadido a un perfil de credenciales de usuario. El nuevo certificado sustituye el certificado existente en el dispositivo.

1. En la barra de menú, 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 una cuenta de usuario.
4. En la sección **Política de TI y perfiles**, en la fila del perfil de credenciales de usuario, haga clic en **Actualizar**.
5. Haga clic en **Examinar** para buscar el archivo de certificado.
6. Escriba una contraseña para el certificado. Para dispositivos iOS, se requiere una contraseña. Para dispositivos Android, no es necesario proporcionar la contraseña en BlackBerry UEM si el dispositivo dispone de la última versión de BlackBerry UEM Client. Si no especifica la contraseña, el usuario debe introducir la contraseña del dispositivo.
7. Haga clic en **Guardar**.

Configuración de un periodo de validez de los certificados de cliente

Si carga certificados a cuentas de usuario individuales para las aplicaciones de BlackBerry Dynamics, debe configurar un periodo de validez de certificados de cliente. Cuando el periodo de validez finaliza, los certificados se eliminan del servidor. Esto evita que un certificado de cliente se quede en el servidor durante un largo periodo después de que se haya cargado en el dispositivo. El tiempo predeterminado es de 24 horas.

Esta función no es compatible en BlackBerry UEM Cloud.

1. En la barra de menú, haga clic en **Configuración > Configuración general > Certificados**.
2. Especifique el periodo de validez para certificados PKCS#12 en el servidor.

Después de terminar: Si aún no lo ha hecho, agregue certificados de cliente a cuentas de usuario.

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