



BlackBerry 2FA

Guía de administración

Contents

Acerca de BlackBerry 2FA.....	5
Arquitectura: BlackBerry 2FA.....	5
Solicitudes de autenticación a través de BlackBerry UEM.....	7
Respuestas de autenticación a través de BlackBerry UEM.....	8
Solicitudes de autenticación a través de BlackBerry UEM Cloud.....	9
Respuestas de autenticación a través de BlackBerry UEM Cloud.....	10
Actualización de BlackBerry UEM.....	10
Perfiles de BlackBerry 2FA.....	11
BlackBerry 2FA para dispositivos administrados con BlackBerry UEM.....	11
BlackBerry 2FA para dispositivos no administrados por BlackBerry UEM.....	11
Identificadores de OTP.....	11
Autenticación previa y autorrescate.....	12
Autenticación directa.....	12
Pasos para gestionar BlackBerry 2FA en BlackBerry UEM	13
Requisitos del sistema: BlackBerry 2FA.....	14
Crear un usuario.....	15
Asignación de la aplicación BlackBerry 2FA a dispositivos con BlackBerry 10.....	16
Crear o modificar un perfil de BlackBerry 2FA en BlackBerry UEM versión 12.8 o anteriores.....	17
Crear o modificar un perfil de BlackBerry 2FA en BlackBerry UEM Cloud o BlackBerry UEM versión 12.9 o posteriores.....	18
Asignar un perfil de BlackBerry 2FA a un grupo.....	21
Creación de un perfil de activación para registrar dispositivos no administrados con BlackBerry 2FA.....	21
Asignación de un perfil de activación de solo registro a un usuario con un dispositivo no administrado....	22
Activar un dispositivo BlackBerry 10.....	22
Activar un dispositivo iOS.....	23
Activar un dispositivo Android.....	23
Activar o cancelar la autenticación previa.....	24
Pasos para administrar identificadores de hardware de contraseña de un solo uso.....	25
Activación de la función de identificadores de OTP.....	25
Desactivación de la función de identificadores de OTP.....	25
Identificadores de hardware de contraseña de un solo uso compatibles.....	25
Uso de la herramienta de conversión del identificador de BlackBerry 2FA.....	26
Modificación del archivo de configuración CSVConfig.....	27
Importación de identificadores de OTP en BlackBerry UEM.....	29
Eliminación de un identificador de OTP de BlackBerry UEM.....	29
Asignación de un identificador de OTP a un usuario.....	29
Eliminación de un identificador de OTP de un usuario.....	29
Adaptación automática de identificadores de hardware no sincronizados.....	30
Resincronización manual de un identificador de hardware.....	30

Registros e informes.....31
 Auditoría de solicitudes de autenticación previa..... 31

Aviso legal..... 33

Acerca de BlackBerry 2FA

BlackBerry 2FA protege el acceso a los recursos críticos de su empresa mediante la autenticación de dos factores. El producto utiliza una contraseña que los usuarios deben introducir, y una solicitud de seguridad en sus dispositivos móviles cada vez que intentan acceder a los recursos. BlackBerry 2FA también es compatible con el uso de identificadores de contraseña de un solo uso (OTP) basados en estándares.

Puede administrar los usuarios de BlackBerry 2FA desde BlackBerry UEM Cloud o la consola de administración de BlackBerry UEM. También puede utilizar BlackBerry 2FA en dispositivos que no están administrados por BlackBerry UEM Cloud ni BlackBerry UEM. BlackBerry 2FA es compatible con dispositivos con iOS y Android que solo tienen un contenedor de BlackBerry Dynamics, dispositivos administrados por sistemas de MDM de terceros y dispositivos no administrados.

Puede utilizar BlackBerry 2FA para proteger una gran variedad de sistemas, incluidos VPN, sistemas compatibles con RADIUS, aplicaciones personalizadas que utilicen una API de REST y servicios en la nube compatibles con SAML que se usen junto con BlackBerry Enterprise Identity.

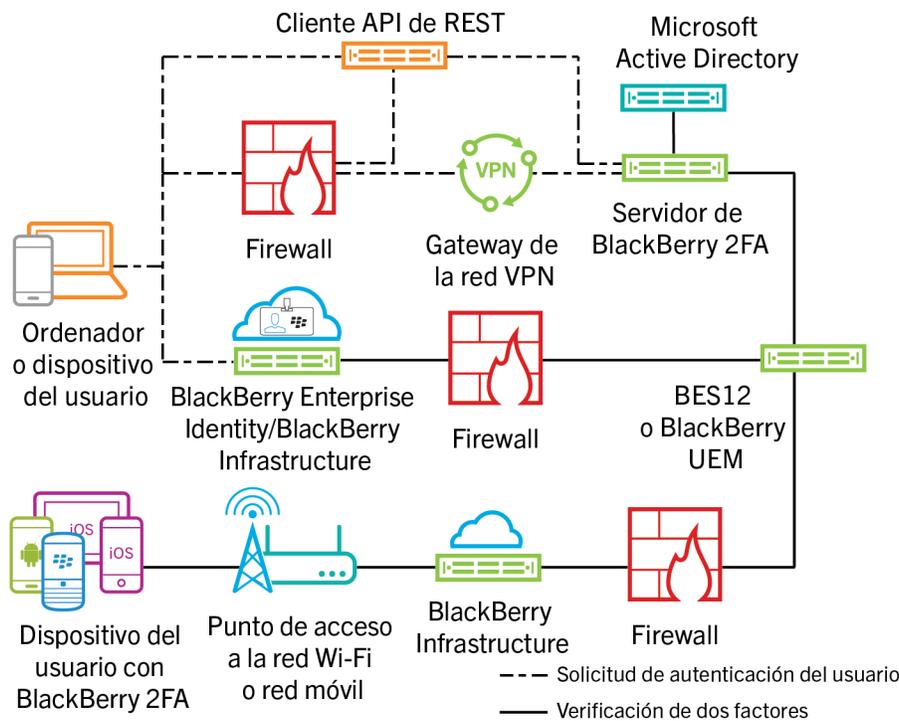
Configurar BlackBerry 2FA para usarse con dispositivos móviles es muy sencillo. El primer factor de autenticación, la contraseña, puede ser el directorio o la contraseña del contenedor del usuario. El segundo factor de autenticación, la solicitud del dispositivo, requiere una aplicación en el dispositivo que desencadene la validación segura del mismo. En los dispositivos con iOS y Android, BlackBerry 2FA se incluye en BlackBerry UEM Client. Se instalan durante la activación, o bien deben ser instalados por los usuarios. En el caso de dispositivos con BlackBerry 10 administrados, debe implementar una aplicación de BlackBerry 2FA, o bien los usuarios deberán tenerla ya instalada.

Configurar BlackBerry 2FA para usuarios sin dispositivos móviles es muy sencillo. Los identificadores de OTP basados en estándares se registran en la consola de BlackBerry UEM y se distribuyen a los usuarios. El primer factor de autenticación es la contraseña de directorio del usuario y el segundo es un código dinámico que aparece en la pantalla del identificador. Para obtener más información, consulte el [contenido de administración de BlackBerry 2FA](#).

El servidor de BlackBerry 2FA es un componente opcional que se implementa cuando el producto se utiliza de forma conjunta con sistemas basados en RADIUS, como la mayoría de las VPN, o bien se utiliza con aplicaciones que llaman a la API de REST del producto. No se requiere el servidor de BlackBerry 2FA en implementaciones que utilizan solo Enterprise Identity, pero puede implementarse en casos en los que desee utilizar la autenticación de dos factores tanto para servicios en la nube como para los otros sistemas compatibles. Para obtener más información, consulte el [contenido de la matriz de compatibilidad del servidor de BlackBerry 2FA](#), el [contenido de instalación y actualización del servidor de BlackBerry 2FA](#) y el [contenido de configuración del servidor de BlackBerry 2FA](#).

Para utilizar BlackBerry 2FA, debe adquirir licencias de usuario de las ediciones Collaboration, Application o Content de BlackBerry Enterprise Mobility Suite, o bien licencias de usuario de 2FA independientes. Para la edición Collaboration, BlackBerry 2FA solo se puede utilizar para la autenticación en aplicaciones de BlackBerry y Microsoft Office 365. Para obtener más información acerca de BlackBerry 2FA, incluido cómo comprar 2FA, consulte blackberry.com.

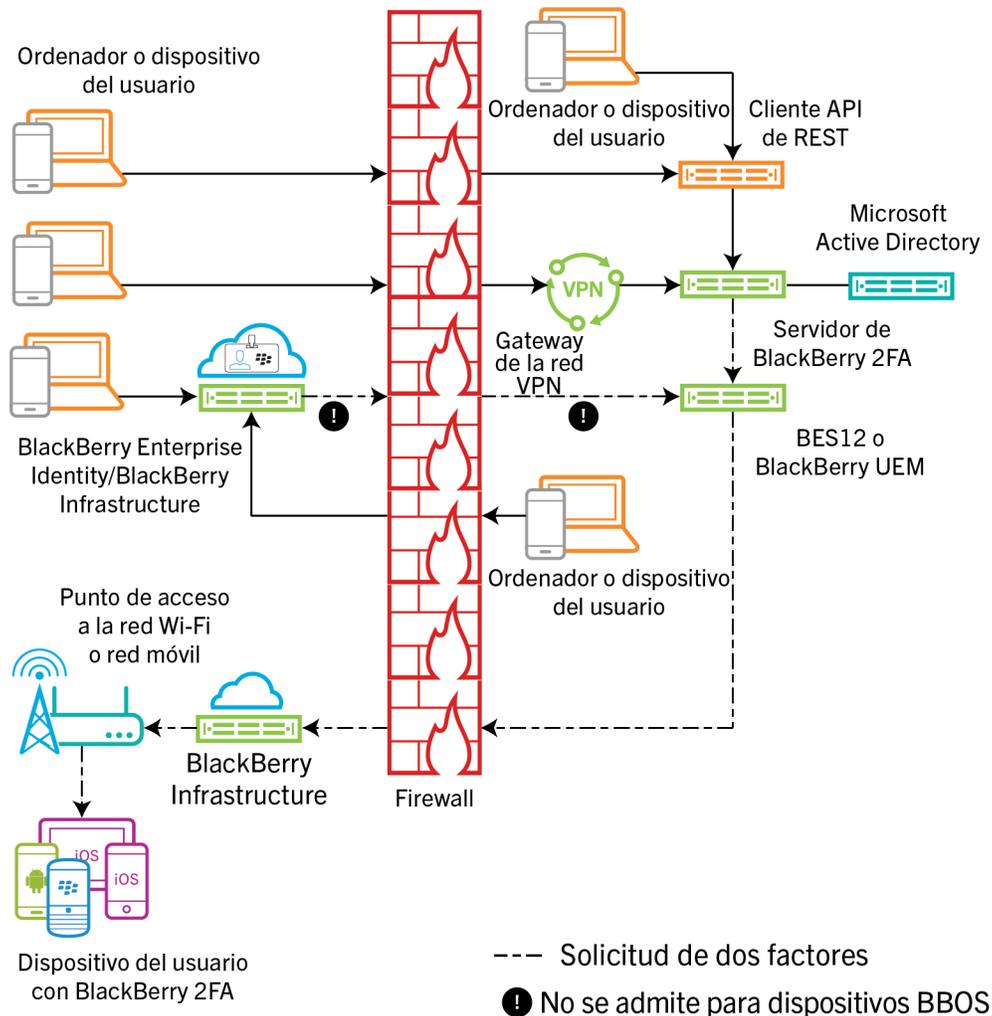
Arquitectura: BlackBerry 2FA



Componente	Descripción
Equipo o dispositivo del usuario	El equipo o dispositivo de un usuario es cualquier equipo o dispositivo, de dentro o fuera del firewall, que se utiliza para establecer la conexión con un recurso que requiere la autenticación en dos fases.
Servidor de BlackBerry 2FA	El servidor de BlackBerry 2FA se conecta a BlackBerry UEM para buscar dispositivos asociados a un usuario y enviar solicitudes de autenticación a la aplicación BlackBerry 2FA instalada en dichos dispositivos.
Gateway de VPN (opcional)	El gateway de la red VPN es un equipo que acepte conexiones VPN a la red de su empresa. Nota: Esta función requiere el servidor de BlackBerry 2FA.
Cliente API de REST (opcional)	El cliente API de REST es un servicio local definido por el cliente que autentica a los usuarios que acceden a él a través de la API de REST del servidor de BlackBerry 2FA. Nota: Esta función requiere el servidor de BlackBerry 2FA.
BlackBerry Enterprise Identity (opcional)	BlackBerry Enterprise Identity ofrece inicio de sesión único (SSO) a servicios en la nube, como Box, Salesforce y G Suite. Enterprise Identity se conecta directamente al servicio BlackBerry 2FA en BlackBerry UEM o BlackBerry UEM Cloud.
BES12 o BlackBerry UEM, BlackBerry UEM Cloud	BlackBerry UEM también administra la configuración de usuario BlackBerry 2FA a través del perfil de BlackBerry 2FA y el uso de identificadores de contraseña de un solo uso (OTP).

Componente	Descripción
Dispositivo del usuario con BlackBerry 2FA	En los dispositivos con iOS y Android, BlackBerry 2FA se incluye en BlackBerry UEM Client. En los dispositivos con BlackBerry 10, los usuarios instalan la aplicación BlackBerry 2FA.

Solicitudes de autenticación a través de BlackBerry UEM



Para iniciar una solicitud de autenticación, el usuario realiza una de las acciones siguientes:

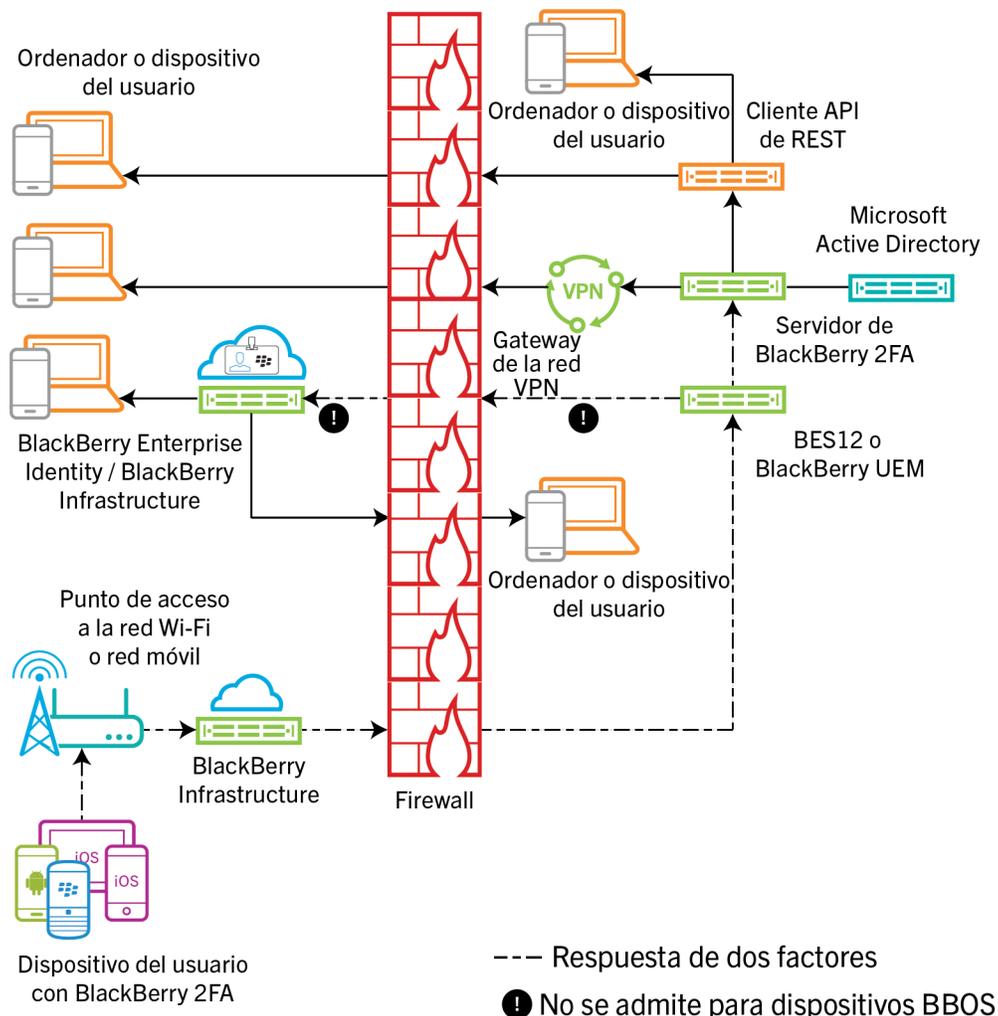
- Accede a la interfaz de inicio de sesión de un servicio personalizado en un equipo o un dispositivo en el trabajo e introduce su información de inicio de sesión
- Accede a la interfaz de inicio de sesión de un servicio personalizado en un equipo o un dispositivo fuera del trabajo e introduce su información de inicio de sesión
- Abre un cliente de VPN en un equipo o un dispositivo fuera del trabajo e introduce su información de inicio de sesión

- Accede a la interfaz de inicio de sesión de un servicio que está configurado para usar BlackBerry Enterprise Identity para la autenticación en un equipo o un dispositivo fuera del trabajo e introduce su información de inicio de sesión
- Accede a la interfaz de inicio de sesión de un servicio que está configurado para usar BlackBerry Enterprise Identity para la autenticación en un equipo o un dispositivo en el trabajo e introduce su información de inicio de sesión

El usuario recibe una solicitud en su dispositivo para confirmar que desea autenticarse. Dependiendo de las opciones de autenticación configuradas para el usuario, puede ser necesario introducir su contraseña de dispositivo o contenedor seguro para poder confirmar la solicitud.

El diagrama no muestra el flujo de datos de las solicitudes de autenticación que usan identificadores de contraseña de un solo uso (OTP).

Respuestas de autenticación a través de BlackBerry UEM

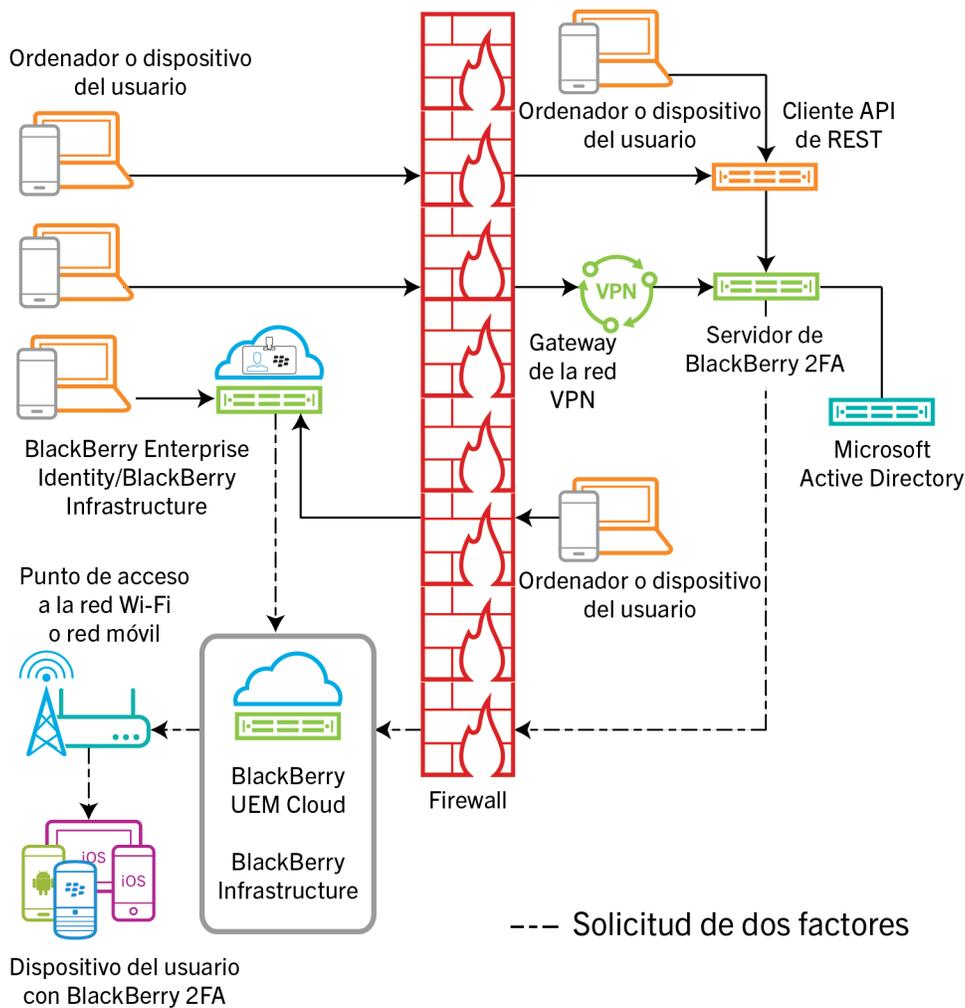


En todas las respuestas mostradas, el usuario confirma la solicitud de autenticación en su dispositivo y la respuesta vuelve a BlackBerry Enterprise Identity o al servidor de BlackBerry 2FA. La contraseña del directorio

se verifica si las opciones de autenticación para el usuario lo requieren. Después de que se verifique, el usuario recibe un mensaje en su dispositivo que indica que la respuesta a la solicitud se ha enviado correctamente.

El diagrama no muestra el flujo de datos de autenticaciones de contraseña mediante identificadores de contraseña de un solo uso (OTP).

Solicitudes de autenticación a través de BlackBerry UEM Cloud



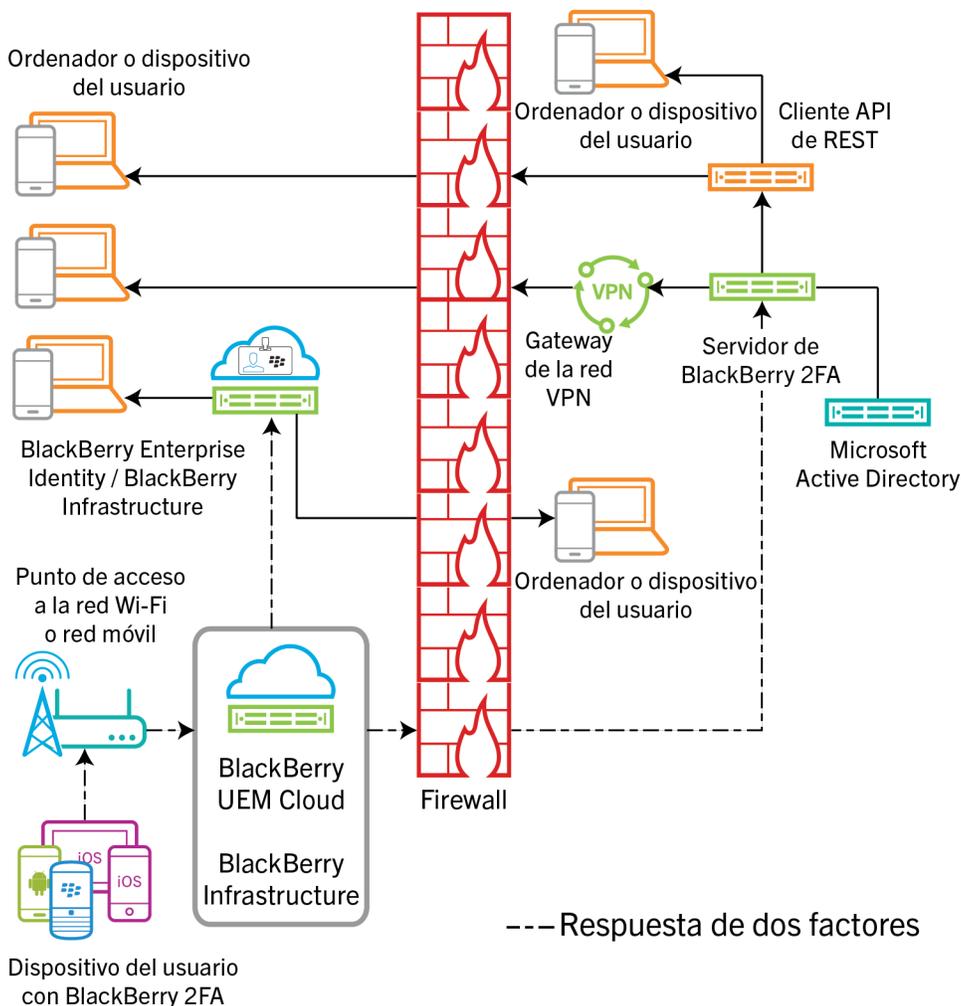
Para iniciar una solicitud de autenticación, el usuario realiza una de las acciones siguientes:

- Accede a la interfaz de inicio de sesión de un servicio que está configurado para usar BlackBerry Enterprise Identity para la autenticación en un equipo o un dispositivo fuera del trabajo e introduce su información de inicio de sesión
- Accede a la interfaz de inicio de sesión de un servicio que está configurado para usar BlackBerry Enterprise Identity para la autenticación en un equipo o un dispositivo en el trabajo e introduce su información de inicio de sesión

El usuario recibe una solicitud en su dispositivo para confirmar que desea autenticarse. Dependiendo de las opciones de autenticación configuradas para el usuario, puede ser necesario introducir su contraseña de dispositivo o contenedor seguro para poder confirmar la solicitud.

El diagrama no muestra el flujo de datos de las solicitudes de autenticación que usan identificadores de contraseña de un solo uso (OTP).

Respuestas de autenticación a través de BlackBerry UEM Cloud



En todas las respuestas mostradas, el usuario confirma la solicitud de autenticación en su dispositivo y la respuesta vuelve a BlackBerry Enterprise Identity. La contraseña del directorio se verifica si las opciones de autenticación para el usuario lo requieren. Después de que se verifique, el usuario recibe un mensaje en su dispositivo que indica que la respuesta a la solicitud se ha enviado correctamente.

El diagrama no muestra el flujo de datos de autenticaciones de contraseña mediante identificadores de contraseña de un solo uso (OTP).

Actualización de BlackBerry UEM

Si actualiza BlackBerry UEM y utiliza un servidor de BlackBerry 2FA, después de la actualización debe reiniciar el servicio de BlackBerry 2FA en el servidor de 2FA. Por ejemplo, si realiza la actualización desde la versión 12.6 a 12.7 de BlackBerry UEM y ejecuta el servidor 2.5 de BlackBerry 2FA, reinicie el servicio BlackBerry 2FA del servidor de 2FA.

Para obtener la última información sobre compatibilidad, consulte la [matriz de compatibilidad del servidor de BlackBerry 2FA](#).

Perfiles de BlackBerry 2FA

Puede utilizar un perfil de BlackBerry 2FA para activar la autenticación para sus usuarios. Para utilizar la versión más reciente de BlackBerry 2FA y sus funciones asociadas, tales como la compatibilidad con identificadores de software de OTP, la compatibilidad con los identificadores de software de OTP, la autenticación directa de BlackBerry 2FA, la autenticación previa de BlackBerry 2FA y el autorrescate, sus usuarios deben tener el perfil de BlackBerry 2FA asignado. Para obtener más información sobre el uso del perfil de BlackBerry 2FA, consulte [Crear o modificar un perfil de BlackBerry 2FA en BlackBerry UEM versión 12.8 o anteriores](#) y [Asignar un perfil de BlackBerry 2FA a un grupo](#). Para obtener información sobre el uso de BlackBerry 2FA en BlackBerry UEM, consulte [Pasos para gestionar BlackBerry 2FA en BlackBerry UEM](#).

BlackBerry 2FA para dispositivos administrados con BlackBerry UEM

Puede activar dispositivos en BlackBerry UEM de forma que pueda administrarlos y utilizar BlackBerry 2FA. Una única tarea de activación proporciona al dispositivo control de MDM y BlackBerry 2FA, lo que simplifica la gestión para los usuarios y los administradores.

Cualquier perfil de activación compatible con BlackBerry UEM permite el uso de BlackBerry 2FA. Para obtener información sobre el uso de BlackBerry 2FA en BlackBerry UEM, consulte el [contenido de administración de BlackBerry 2FA](#).

BlackBerry 2FA para dispositivos no administrados por BlackBerry UEM

Si la administración de BlackBerry UEM no es una opción, o un dispositivo ya está siendo administrado por otra solución de MDM, puede activar dispositivos con BlackBerry UEM para que utilicen únicamente BlackBerry 2FA.

Los dispositivos activados de esta forma no se administran con BlackBerry UEM. No se crea ningún espacio de trabajo en los dispositivos, no se establece ningún control administrativo del dispositivo, no se proporciona seguridad adicional para los datos de trabajo y se mantiene la privacidad de los datos personales de los usuarios.

Esta opción está disponible únicamente para dispositivos iOS y Android. Para obtener información sobre el uso de BlackBerry 2FA en BlackBerry UEM, consulte el [contenido de administración de BlackBerry 2FA](#).

Identificadores de OTP

BlackBerry UEM es compatible con el uso de los identificadores de contraseña de un solo uso (OTP) a través del servicio BlackBerry 2FA. Los identificadores de OTP ofrecen un esquema de autenticación seguro para aquellos usuarios que no tienen un dispositivo móvil o cuyo dispositivo móvil no dispone de conectividad suficiente para admitir notificaciones de dispositivos de BlackBerry 2FA en tiempo real. Cuando se utiliza una OTP en lugar de una notificación de dispositivo como segundo factor de autenticación, la OTP se proporciona a través del mismo canal que la contraseña del usuario y su dispositivo móvil no se señala.

Puede introducir el código OTP con el nombre de usuario o la contraseña.

- Cuando utilice un código OTP con el nombre de usuario, después del nombre de usuario, escriba una coma (,) y, a continuación, el código OTP sin espacios entre ellos. Por ejemplo, si el nombre de usuario es "janedoe" y el código es "555123", se debe introducir como "janedoe,555123". Con este método, los usuarios pueden verificar fácilmente el código que han introducido.
- Cuando se utiliza un código OTP con la contraseña, el código precede a la contraseña del usuario. Por ejemplo, si el código es "555123" y la contraseña es "AbCdeF", debe introducirse como "555123AbCdeF".

Identificadores de software

Active los identificadores de OTP del software para los usuarios en el perfil de BlackBerry 2FA que les haya asignado. El identificador de software se puede encontrar en la aplicación BlackBerry UEM Client desplazándose a través de la pantalla de inicio.

Identificadores de hardware

Para administrar identificadores de OTP de hardware en BlackBerry UEM, el usuario debe tener un perfil de BlackBerry 2FA asignado.

Para obtener más información sobre los últimos identificadores de hardware compatibles, consulte la [matriz de compatibilidad del servidor de BlackBerry 2FA](#).

Autenticación previa y autorrescate

La autenticación previa de BlackBerry 2FA y el autorrescate son funciones que permiten a los usuarios autenticarse en los recursos de su empresa durante un período predeterminado con un solo factor. Estas funciones se activan y configuran de forma independiente.

La autenticación previa se debe utilizar cuando el usuario prevé no tener acceso al dispositivo o no hay cobertura de red durante un breve periodo de tiempo (por ejemplo, cuando está en un avión). Los usuarios pueden solicitar la autenticación previa desde el dispositivo o los administradores pueden activarla a través de la consola de administración de BlackBerry UEM. BlackBerry recomienda usar la función de OTP de software siempre que sea posible, porque retiene la seguridad completa de dos factores, aunque no sea tan fácil de usar.

El autorrescate se debe utilizar cuando un usuario ha perdido el dispositivo o no tiene acceso al dispositivo durante un período de tiempo más largo que un día o más (por ejemplo, el usuario pierde el dispositivo y espera un reemplazo). Los usuarios pueden acceder a la función de autorrescate desde BlackBerry UEM Self-Service, lo que significa que solo se puede activar si el usuario está conectado a la red de la empresa.

Autenticación directa

Puede activar la autenticación directa de BlackBerry 2FA para que, cuando los usuarios deseen autenticar los recursos de su empresa, comiencen el proceso de autenticación desde sus dispositivos, en lugar de recibir una solicitud de confirmación y tener que utilizar una contraseña de un solo uso. Cuando active la función de autenticación directa de los usuarios, estos deben utilizar la contraseña de directorio para iniciar sesión en los recursos de su empresa en el plazo que haya especificado.

Los usuarios pueden acceder a la función de autenticación directa desde BlackBerry UEM Client en dispositivos con Android y iOS, y la aplicación BlackBerry 2FA en dispositivos con BlackBerry 10.

Pasos para gestionar BlackBerry 2FA en BlackBerry UEM

Para usar BlackBerry UEM para gestionar BlackBerry 2FA, debe realizar las siguientes acciones:

Paso	Acción
1	Verifique que su entorno cumple los requisitos del servidor y del dispositivo. Para obtener más información, consulte Requisitos del sistema: BlackBerry 2FA .
2	De forma opcional, instale y configure el servidor de BlackBerry 2FA. Para obtener más información, consulte el contenido de instalación y configuración .
3	Crear un usuario.
4	Asignación de la aplicación BlackBerry 2FA a dispositivos con BlackBerry 10.
5	Crear o modificar un perfil de BlackBerry 2FA en BlackBerry UEM versión 12.8 o anteriores o bien, Crear o modificar un perfil de BlackBerry 2FA en BlackBerry UEM Cloud o BlackBerry UEM versión 12.9 o posteriores.
6	Asignar un perfil de BlackBerry 2FA a un grupo.
7	De forma opcional, Creación de un perfil de activación para registrar dispositivos no administrados con BlackBerry 2FA.
8	De forma opcional, Asignación de un perfil de activación de solo registro a un usuario con un dispositivo no administrado.
9	Activar un dispositivo BlackBerry 10.
10	Activar un dispositivo iOS.
11	Activar un dispositivo Android.
12	Activar o cancelar la autenticación previa.
13	De forma opcional, configure BlackBerry UEM para usar identificadores de contraseña de un solo uso (OTP). Para obtener más información, consulte Pasos para administrar identificadores de hardware de contraseña de un solo uso .

Requisitos del sistema: BlackBerry 2FA

Para poder usar BlackBerry UEM para administrar BlackBerry 2FA, debe asegurarse de que se cumplan los siguientes requisitos:

Elemento	Requisito
BlackBerry UEM o BlackBerry UEM Cloud	<p>Una de las siguientes:</p> <ul style="list-style-type: none">• BlackBerry UEM versión 12.6 o posterior• BlackBerry UEM Cloud <p>Para obtener más información sobre la instalación de BlackBerry UEM 12.6 o posterior, consulte el contenido de instalación y actualización de BlackBerry UEM.</p>
Servidor de BlackBerry 2FA	<ul style="list-style-type: none">• Versión 2.0 o posterior (versión 2.5 para la integración completa de todas las nuevas funciones de BlackBerry UEM, incluidos los identificadores de OTP) <p>Para obtener más información sobre los requisitos del sistema, consulte el contenido de la matriz de compatibilidad de BlackBerry 2FA.</p> <p>Nota: Para administrar el servidor de BlackBerry 2FA desde la consola de administración BlackBerry UEM, el servidor BlackBerry 2FA requiere la versión 2.5.</p>
Licencias de BlackBerry 2FA	<ul style="list-style-type: none">• BlackBerry 2FA se incluye en BlackBerry Enterprise Mobility Suite - Application Edition y BlackBerry Enterprise Mobility Suite - Content Edition, y también se puede adquirir por separado.• BlackBerry 2FA se incluye en BlackBerry Enterprise Mobility Suite - Collaboration Edition para la autenticación solo en los productos de propiedad empresarial de Microsoft Office 365 y BlackBerry.• BlackBerry 2FA se incluye en todas las licencias de BlackBerry Workspaces independientes solo para la autenticación de Workspaces.• Póngase en contacto con su representante de cuenta de BlackBerry para obtener la información más reciente sobre empaquetado, precios y licencias.
BlackBerry 10	<ul style="list-style-type: none">• Todas las versiones. Para obtener más información, consulte el contenido de la matriz de compatibilidad de BlackBerry 2FA.
iOS	<ul style="list-style-type: none">• iOS 8 y posterior. Para obtener más información, consulte el contenido de la matriz de compatibilidad de BlackBerry 2FA.• Última versión de BlackBerry UEM Client instalada. Para obtener más información, consulte el contenido de administración de BlackBerry UEM.
Android	<ul style="list-style-type: none">• Android 4.0.x y posterior. Para obtener más información, consulte el contenido de la matriz de compatibilidad de BlackBerry 2FA.• Última versión de BlackBerry UEM Client instalada. Para obtener más información, consulte el contenido de administración de BlackBerry UEM.

Elemento	Requisito
Licencias de dispositivo	No se requieren licencias para dispositivos que usen BlackBerry 2FA pero que estén gestionados por BlackBerry UEM.

Crear un usuario

Cada usuario de BlackBerry 2FA debe existir como usuario en BlackBerry UEM. Lleve a cabo una de estas acciones:

- Si el usuario ya está en BlackBerry UEM, siga las instrucciones para establecer una contraseña de activación y enviar un mensaje de correo de activación, según se indica en el [contenido de administración de BlackBerry UEM](#).
- Si el usuario todavía no está en BlackBerry UEM, siga estos pasos para crear una cuenta y enviarle una contraseña de activación.

Si desea acceder a los ajustes avanzados, siga las instrucciones para crear una cuenta de usuario, según se indica en el [contenido de administración de BlackBerry UEM](#).

1. En la consola de administración de BlackBerry UEM, en la barra de menú, haga clic en **Usuarios**.
2. En el panel izquierdo, haga clic en **Agregar usuario**.
3. Lleve a cabo una de estas acciones:

Tarea	Pasos
Agregue un usuario de directorio.	<ol style="list-style-type: none"> a. En la pestaña Directorio de la empresa, en el campo de búsqueda, especifique los criterios de búsqueda para el usuario de directorio que desea agregar. Puede buscar por nombre, apellidos, nombre para mostrar, nombre de usuario o dirección de correo. b. Haga clic en . c. En los resultados de la búsqueda, seleccione la cuenta de usuario.
Agregue un usuario local.	<ol style="list-style-type: none"> a. Haga clic en la pestaña Local. b. Escriba el Nombre y los Apellidos de la cuenta de usuario. c. En el campo Nombre para mostrar, realice los cambios que sean necesarios. El nombre para mostrar se configura automáticamente con el nombre y los apellidos que se han especificado. d. En el campo Nombre de usuario, introduzca un nombre de usuario exclusivo para la cuenta de usuario. e. En el campo Dirección de correo, introduzca una dirección de correo de contacto para la cuenta de usuario. Se necesita una dirección de correo electrónico para la cuenta de usuario a fin de activar un servicio como, por ejemplo, BlackBerry Workspaces o la administración de dispositivos. f. En el campo Contraseña de la consola, introduzca una contraseña para BlackBerry UEM Self-Service. Si el usuario tiene asignada una función administrativa, también pueden usar la contraseña para acceder a la consola de gestión.

4. Lleve a cabo una de las tareas siguientes:

Tarea	Pasos
Genere automáticamente una contraseña de activación para el usuario y envíe un correo de activación.	<ol style="list-style-type: none"> Seleccione la opción Generar automáticamente la contraseña de activación del dispositivo y enviar un correo electrónico con las instrucciones de activación. En el campo Caducidad del periodo de activación, especifique el número de minutos, las horas o los días en los que el usuario puede activar un dispositivo antes de que caduque la contraseña de activación. En la lista desplegable Plantilla del correo de activación, haga clic en la plantilla que desea utilizar para correo de activación.
Establezca una contraseña de activación para el usuario y, opcionalmente, envíe un correo de activación.	<ol style="list-style-type: none"> Seleccione la opción Establecer contraseña de activación del dispositivo. Escriba una contraseña de activación. En el campo Caducidad del periodo de activación, especifique el número de minutos, las horas o los días en los que el usuario puede activar un dispositivo antes de que caduque la contraseña de activación. Lleve a cabo una de las siguientes acciones: <ol style="list-style-type: none"> Para enviar instrucciones de activación al usuario, en la lista desplegable Plantilla del correo de activación, haga clic en una plantilla que se utilizará en el correo de activación. Si no desea enviar instrucciones de activación para el usuario, desactive la casilla de verificación Enviar un correo electrónico con las instrucciones y la contraseña de activación. Debe comunicar la contraseña de activación al usuario.
No establezca una contraseña de activación para el usuario.	<ol style="list-style-type: none"> Seleccione la opción No establecer contraseña de activación del dispositivo. Puede establecer una contraseña de activación y enviar un correo de activación más tarde.

- Si utiliza variables personalizadas, amplíe **Variables personalizadas** y especifique los valores apropiados para las variables que se han definido.
- Lleve a cabo una de las siguientes acciones:
 - Para guardar el usuario, haga clic en **Guardar**.
 - Para guardar el usuario y crear otra cuenta de usuario, haga clic en **Guardar y crear nueva**.

Asignación de la aplicación BlackBerry 2FA a dispositivos con BlackBerry 10

Debe realizar la siguiente tarea para asignar la aplicación a dispositivos con BlackBerry 10 cuando utilice BlackBerry UEM. Para obtener más información sobre la asignación de aplicaciones, consulte el [contenido de administración de BlackBerry UEM](#).

- Descargue la aplicación de <https://swdownloads.blackberry.com/Downloads/entry.do?code=0C52D419A421FB13BB58357E67B7FB4B> y copie el archivo .bar en una ubicación a la que pueda acceder la consola de administración de BlackBerry UEM.

2. Si es necesario, utilice la consola de administración de BlackBerry UEM para especificar una ubicación de red compartida para aplicaciones internas.
3. En la consola de administración de BlackBerry UEM, agregue el archivo .bar como aplicación interna.
4. En la consola de administración de BlackBerry UEM, asigne la app a usuarios o a grupos.

La aplicación se instala automáticamente en cualquier dispositivo con BlackBerry 10 que el usuario active con un espacio de trabajo.

Crear o modificar un perfil de BlackBerry 2FA en BlackBerry UEM versión 12.8 o anteriores

Para utilizar BlackBerry 2FA, debe crear un perfil de BlackBerry 2FA y asignarlo a los usuarios.

1. En la barra de menú, haga clic en **Políticas y perfiles**.
2. Haga clic en **Redes y conexiones > BlackBerry 2FA**.
3. Lleve a cabo una de estas acciones:
 - Para crear un perfil, haga clic en .
 - Para modificar un perfil, haga clic en el nombre del perfil que desea modificar y haga clic en .
4. Escriba un nombre para el perfil de BlackBerry 2FA.
5. También puede agregar una descripción para el perfil de BlackBerry 2FA.
6. Seleccione una opción de autenticación:
 - a) Seleccione **Autenticación en dos fases** si desea crear un perfil de BlackBerry 2FA estándar.
 - b) Seleccione **Autenticación de factor único mediante contraseña de empresa** si desea crear un perfil para usuarios que no tienen un dispositivo pero necesitan acceder a los recursos de su organización. Esta opción es menos segura, ya que el usuario proporciona solo una contraseña de directorio cuando solicita la autenticación y no se envía una solicitud de confirmación para la misma. Los identificadores de contraseña de un solo uso (OTP) no son compatibles con esta opción.
7. Seleccione una contraseña para usarla cuando el dispositivo lo solicite:
 - a) Seleccione la opción **Contraseña de empresa** si desea crear un perfil para usuarios que primero necesitan proporcionar una contraseña de directorio cuando solicitan la autenticación y, a continuación, recibir una solicitud de confirmación en sus dispositivos.
 - b) Seleccione la opción **Contraseña de dispositivo pasiva** si desea crear un perfil para usuarios de BlackBerry 10 que deben recibir una solicitud pasiva para proporcionar la contraseña de su espacio de trabajo con el fin de desbloquearlo y, a continuación, recibir una solicitud de confirmación para la autenticación en sus dispositivos. La solicitud pasiva significa que los usuarios no necesitan proporcionar una contraseña para el espacio de trabajo si el espacio de trabajo del dispositivo ya está desbloqueado al solicitar la autenticación.
 - c) Seleccione la opción **Contraseña de dispositivo activa** si desea crear un perfil para usuarios de BlackBerry 10 que deben recibir una solicitud activa para proporcionar la contraseña de su espacio de trabajo con el fin de desbloquearlo y, a continuación, recibir una solicitud de confirmación para la autenticación en sus dispositivos. La solicitud activa significa que los usuarios deben proporcionar una contraseña para el espacio de trabajo si el espacio de trabajo del dispositivo ya está desbloqueado al solicitar la autenticación.
8. Además, si utiliza la política de autenticación **Contraseña de empresa**, realice cualquier de las acciones siguientes:
 - a) Para permitir a los usuarios que utilicen OTP en la aplicación BlackBerry UEM Client, seleccione **Permitir identificadores de contraseñas de un solo uso**. Especifique la longitud de las OTP que se generan.

- b) Para permitir a los usuarios que soliciten la autenticación directa, seleccione **Permitir autenticación directa desde el dispositivo del usuario**. Especifique el tiempo, en segundos, que los usuarios tienen para completar el proceso de autenticación de dos factores después de que lo hayan iniciado en su dispositivo móvil. La configuración máxima es "180".
 - c) Para permitir a los usuarios que establezcan un periodo de autorrescate, seleccione **Permitir el autorrescate desde BlackBerry UEM Self-Service**. Especifique, en horas, el tiempo predeterminado y el tiempo máximo durante el que los usuarios pueden acceder a los recursos de su empresa sin necesidad de responder a una solicitud de confirmación en sus dispositivos.
 - d) Para permitir a los usuarios que establezcan un período de autenticación previa, seleccione **Permitir autenticación previa desde el dispositivo del usuario**. Especifique, en horas, el tiempo predeterminado y el tiempo máximo durante el que los usuarios pueden acceder a los recursos de su empresa sin necesidad de responder a una solicitud de confirmación en sus dispositivos (la solicitud no aparecerá).
9. Haga clic en **Agregar** o **Guardar**.

Crear o modificar un perfil de BlackBerry 2FA en BlackBerry UEM Cloud o BlackBerry UEM versión 12.9 o posteriores

Para utilizar BlackBerry 2FA, debe crear un perfil de BlackBerry 2FA y asignarlo a los usuarios.

1. En la barra de menú, haga clic en **Políticas y perfiles**.
2. Haga clic en **Redes y conexiones > BlackBerry 2FA**.
3. Lleve a cabo una de estas acciones:
 - Para crear un perfil, haga clic en .
 - Para modificar un perfil, haga clic en el nombre del perfil que desea modificar y haga clic en .
4. Escriba un nombre para el perfil de BlackBerry 2FA.
5. También puede agregar una descripción para el perfil de BlackBerry 2FA.
6. Lleve a cabo una de estas acciones:
 - a) Seleccione **Autenticar con BlackBerry 2FA** si desea crear un perfil de BlackBerry 2FA estándar.
 - b) Seleccione **Autenticar solo con contraseña de empresa** si desea crear un perfil para usuarios que no tienen un dispositivo pero necesitan acceder a los recursos de su empresa. Esta opción es menos segura, ya que el usuario proporciona solo una contraseña de directorio cuando solicita la autenticación y no se envía una solicitud de confirmación para la misma. Los identificadores de contraseña de un solo uso (OTP) no son compatibles con esta opción.
7. Si ha seleccionado el modo de autenticación "Autenticar con BlackBerry 2FA", configure los siguientes ajustes:

Configuración	Descripción
Permitir autenticación de inserción	Esta configuración especifica si se permite a los usuarios autenticarse utilizando la solicitud de confirmación de 2FA en su dispositivo.
Requerir contraseña de empresa	Esta configuración especifica si los usuarios deben proporcionar su contraseña de empresa al iniciar sesión en los recursos de su empresa. Después de que un usuario introduce su contraseña, se le solicita que se autentique en su dispositivo.

Configuración	Descripción
	Esta configuración solo es válida si se ha seleccionado Permitir autenticación de inserción.
Permitir autenticación previa desde dispositivos móviles	<p>Esta configuración especifica si se permite a los usuarios utilizar la función de autenticación previa para autenticarse en los recursos de su organización durante un periodo breve predeterminado. Si selecciona esta opción, la función está disponible para los usuarios en la pantalla de inicio de la aplicación BlackBerry UEM Client.</p> <p>Especifique la duración predeterminada y máxima, en horas, que los usuarios pueden acceder a los recursos de su organización sin que se les solicite que se autentifiquen en su dispositivo.</p> <p>Esta configuración es válida solo si se han seleccionado Permitir autenticación de inserción y Requerir contraseña de empresa.</p>
Requerir contraseña del dispositivo si el dispositivo está bloqueado	<p>Esta configuración especifica si los usuarios deben desbloquear su dispositivo antes de poder responder a la solicitud de autenticación en el dispositivo.</p> <p>Esta configuración solo es válida si se ha seleccionado Permitir autenticación de inserción.</p>
Requerir nueva introducción de contraseña del dispositivo si el dispositivo ya está desbloqueado (solo dispositivos con BlackBerry 10)	<p>Esta configuración especifica si los usuarios de dispositivos con BlackBerry 10 deben introducir la contraseña de su dispositivo incluso aunque el dispositivo ya esté desbloqueado, antes de poder responder a la solicitud de autenticación en el dispositivo.</p> <p>Esta configuración es válida solo si se han seleccionado Permitir autenticación de inserción y Requerir contraseña del dispositivo si el dispositivo está bloqueado.</p>
Permitir autenticación directa desde dispositivos móviles	<p>Esta configuración especifica si se permite a los usuarios utilizar la función de autenticación directa para iniciar el proceso de autenticación en su dispositivo móvil. Si selecciona esta opción, la función está disponible para los usuarios en la pantalla de inicio de la aplicación BlackBerry UEM Client.</p> <p>Debe especificar la duración, en segundos, en la que los usuarios deben completar el proceso de autenticación de dos factores. La configuración</p>

Configuración	Descripción
	<p>predeterminada es "120" y la configuración máxima es "180".</p> <p>Esta configuración solo es válida si se ha seleccionado Permitir autenticación de inserción.</p>
Permitir autenticación con contraseña de un solo uso (OTP)	Esta configuración especifica si se permite a los usuarios utilizar códigos OTP como segundo factor de autenticación.
Requerir contraseña de empresa	<p>Esta configuración especifica si el usuario debe introducir su contraseña del directorio junto con el código OTP.</p> <p>Esta configuración es válida solo si se ha seleccionado Permitir la autenticación con contraseñas de un solo uso (OTP).</p>
Permitir generación de OTP en dispositivos móviles	<p>Esta configuración especifica si se generan códigos OTP en su dispositivo móvil. Si selecciona esta opción, los usuarios pueden utilizar los códigos OTP que se muestran en la pantalla de inicio de la aplicación BlackBerry UEM Client.</p> <p>Especifique la longitud de los códigos OTP que desea que se generen en UEM Client. La longitud predeterminada es "6".</p> <p>Esta configuración es válida solo si se ha seleccionado Permitir la autenticación con contraseñas de un solo uso (OTP).</p>
Permitir identificadores de OTP de hardware	<p>Esta configuración especifica si se permite a los usuarios utilizar identificadores de OTP de hardware. Si selecciona esta opción, los usuarios pueden utilizar códigos OTP en los identificadores de hardware que tengan asignados.</p> <p>Esta configuración es válida solo si se ha seleccionado Permitir la autenticación con contraseñas de un solo uso (OTP).</p>
Permitir el autorrescate desde BlackBerry UEM Self-Service	<p>Esta configuración especifica si se permite a los usuarios utilizar la función de autorrescate para autenticarse en los recursos de su organización durante un periodo predeterminado. Si selecciona esta opción, los usuarios pueden acceder a la función de autorrescate desde BlackBerry UEM Self-Service, al que los usuarios pueden acceder solo si están conectados a la red de la empresa.</p> <p>Especifique la duración predeterminada y máxima, en horas, que los usuarios pueden acceder a los</p>

Configuración	Descripción
	recursos de su organización sin que se les solicite que se autenticquen en su dispositivo.

8. Haga clic en **Agregar** o **Guardar**.

Asignar un perfil de BlackBerry 2FA a un grupo

Un usuario debe tener un perfil de BlackBerry 2FA asignado para utilizar BlackBerry 2FA.

Antes de empezar:

- [Crear o modificar un perfil de BlackBerry 2FA en BlackBerry UEM versión 12.8 o anteriores.](#)
 - [Crear o modificar un perfil de BlackBerry 2FA en BlackBerry UEM Cloud o BlackBerry UEM versión 12.9 o posteriores.](#)
1. En la consola de gestión de la barra de menú, haga clic en **Usuarios**.
 2. Busque un usuario.
 3. En los resultados de la búsqueda, haga clic en el nombre del usuario.
 4. En la sección **Política de TI y perfiles**, haga clic en **+**.
 5. Haga clic en **BlackBerry 2FA**.
 6. En la lista desplegable **Perfil de BlackBerry 2FA**, haga clic en un perfil de BlackBerry 2FA.
 7. Si el tipo de perfil que ha seleccionado en el paso 6 ya está asignado directamente al usuario, haga clic en **Sustituir**. De lo contrario, haga clic en **Asignar**.

Creación de un perfil de activación para registrar dispositivos no administrados con BlackBerry 2FA

Realice la siguiente tarea para crear un perfil de activación para usuarios con dispositivos no administrados con BlackBerry UEM. Estos dispositivos deben registrarse a través de BlackBerry UEM, de modo que puedan utilizarse con BlackBerry 2FA. Este tipo de activación se aplica únicamente a dispositivos iOS y Android.

1. En la consola de administración de BlackBerry UEM, en la barra de menú, haga clic en **Políticas y perfiles**.
2. Haga clic en **+** al lado de **Activación**.
3. Escriba un nombre y una descripción para el perfil.
4. En el campo **Número de dispositivos que un usuario puede activar**, especifique el número máximo de dispositivos que el usuario puede activar.
5. En la lista desplegable **Propietario del dispositivo**, lleve a cabo una de las siguientes acciones:
 - Si algunos usuarios activan dispositivos personales y algunos usuarios activan los dispositivos de trabajo, seleccione **No especificado**.
 - Si los usuarios suelen activar los dispositivos de trabajo, seleccione **Trabajo**.
 - Si los usuarios suelen activar dispositivos personales, seleccione **Personal**.
6. Opcionalmente, seleccione un aviso de la empresa en la lista desplegable **Asignar aviso de la organización**. Si asigna un aviso de la empresa, los usuarios que activen los dispositivos iOS deberán aceptar el aviso para completar la activación.

7. En la sección **Tipos de dispositivo que los usuarios pueden activar**, seleccione los tipos de dispositivo iOS y Android.
8. Haga clic en las pestañas **iOS** o **Android** y realice las siguientes acciones:
 - En la lista desplegable **Restricciones de modelo de dispositivo**, seleccione si solo desea permitir los dispositivos especificados o prefiere no poner restricciones sobre los tipos de dispositivo. Si elige una opción distinta de **Sin restricciones**, haga clic en **Editar**, seleccione los dispositivos que desee restringir o permitir y, a continuación, haga clic en **Guardar**.
 - En la lista desplegable **Versión permitida**, seleccione la versión mínima permitida.
 - En la sección **Tipo de activación**, seleccione **Registro de dispositivo solo para BlackBerry 2FA**.
9. Haga clic en **Agregar**.

Asignación de un perfil de activación de solo registro a un usuario con un dispositivo no administrado

Realice la siguiente tarea para asignar un perfil de activación a usuarios con dispositivos no administrados con BlackBerry UEM. Estos dispositivos deben registrarse a través de BlackBerry UEM, de modo que puedan utilizarse con BlackBerry 2FA. Este tipo de activación solo está disponible para dispositivos iOS y Android.

Antes de empezar:

- [Creación de un perfil de activación para registrar dispositivos no administrados con BlackBerry 2FA](#).
1. En la consola de gestión de BlackBerry UEM, en la barra de menú, haga clic en **Usuarios**.
 2. Busque un usuario.
 3. En los resultados de la búsqueda, haga clic en el nombre del usuario.
 4. En la sección **Política de TI y perfiles**, haga clic en **+**.
 5. Haga clic en **Activación**.
 6. En la lista desplegable **Perfil de activación**, haga clic en el perfil de activación que ha creado para permitir el registro de dispositivos no administrados para su uso con BlackBerry 2FA.
 7. Si el perfil que ha seleccionado en el paso 6 ya está asignado directamente al usuario, haga clic en **Sustituir**. De lo contrario, haga clic en **Asignar**.

Activar un dispositivo BlackBerry 10

Envíe las instrucciones de activación siguientes al usuario del dispositivo.

1. En el dispositivo, diríjase a **Configuración**.
2. Toque **Cuentas**.
3. Si tiene cuentas en este dispositivo, toque **Agregar cuenta**. De lo contrario, continúe con el paso 4.
4. Toque **Correo, calendario y contactos**.
5. Escriba su dirección de correo de trabajo y toque **Siguiente**.
6. En el campo **Contraseña**, escriba la contraseña de activación que recibió. Toque **Siguiente**.
7. Si recibe una advertencia de que el dispositivo no puede consultar la información de conexión, realice los siguientes pasos:
 - a) Toque **Avanzado**.
 - b) Toque **Cuenta de trabajo**.

- c) En el campo **Dirección del servidor**, escriba la dirección del servidor. Puede encontrar la dirección del servidor en el mensaje de correo de activación que ha recibido o en BlackBerry UEM Self-Service.
- d) Toque **Hecho**.

8. Siga las instrucciones que aparecen en pantalla para completar el proceso de activación.

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

- En el dispositivo, diríjase al BlackBerry Hub y confirme que aparece la dirección de correo. Vaya al calendario y confirme que aparecen las citas.
- En BlackBerry UEM Self-Service, compruebe que el dispositivo aparezca como un dispositivo activado. El estado puede tardar hasta dos minutos en actualizarse una vez que haya activado el dispositivo.
- Verifique la aplicación BlackBerry 2FA, que se descarga y se instala automáticamente en el dispositivo del usuario, comprobando su espacio de trabajo. Si no lo está, la aplicación BlackBerry 2FA puede descargarse de BlackBerry World para el trabajo.

Activar un dispositivo iOS

Envíe las instrucciones de activación siguientes al usuario del dispositivo.

1. Instale el BlackBerry UEM Client en el dispositivo. Puede descargar este elemento desde Apple App Store.
2. En el dispositivo, toque **BlackBerry UEM**.
3. Lea el contrato de licencia y toque **Acepto**.
4. Escriba su dirección de correo de trabajo y toque **Go**.
5. Si es necesario, escriba la dirección del servidor y toque **Go**. Puede encontrar la dirección del servidor en el mensaje de correo de activación que ha recibido o en BlackBerry UEM Self-Service.
6. Confirme que los detalles del certificado mostrados en el dispositivo son correctos y toque **Aceptar**. Si su administrador le envió los detalles del certificado por separado, puede comparar la información que se muestra con la información que recibió.
7. Escriba la contraseña de activación y toque **Activar mi dispositivo**.
8. Toque **Aceptar** para instalar el certificado necesario.
9. Siga las instrucciones que aparecen en pantalla para completar la instalación.
10. Si se le solicita introducir la contraseña de su cuenta de correo electrónico o el código secreto de su dispositivo, siga las instrucciones que aparecen en la pantalla.

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

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

Activar un dispositivo Android

Envíe las instrucciones de activación siguientes al usuario del dispositivo.

1. Instale el BlackBerry UEM Client en el dispositivo. Puede descargar BlackBerry UEM Client desde Google Play.
2. En el dispositivo, toque **BlackBerry UEM**.

3. Lea el contrato de licencia y toque **Acepto**.
4. Escriba su dirección de correo de trabajo y toque **Siguiente**.
5. Si es necesario, escriba la dirección del servidor y toque **Siguiente**. Puede encontrar la dirección del servidor en el mensaje de correo de activación que ha recibido o en BlackBerry UEM Self-Service.
6. Confirme que los detalles del certificado mostrados en el dispositivo son correctos y toque **Aceptar**. Si su administrador le envió los detalles del certificado por separado, puede comparar la información que se muestra con la información que recibió.
7. Escriba la contraseña de activación y toque **Activar mi dispositivo**.
8. Toque **Siguiente**.
9. Toque **Activar**.

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

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

Activar o cancelar la autenticación previa

Realice la siguiente tarea si su empresa controla la autenticación previa de BlackBerry 2FA a través de peticiones de servicio de TI, o si desea anular la configuración de autenticación previa existente para un usuario.

Antes de empezar:

- Compruebe que el usuario tiene un perfil de BlackBerry 2FA asignado.
1. En la consola de gestión de BlackBerry UEM, en la barra de menú, haga clic en **Usuarios**.
 2. Busque un usuario.
 3. En los resultados de la búsqueda, haga clic en el nombre del usuario.
 4. En el resumen del usuario, haga clic en **Activar omisión de BlackBerry 2FA**.
 5. En el cuadro de diálogo **Establezca el periodo de omisión**, especifique, en horas, el tiempo durante el que los usuarios pueden acceder a los recursos de su empresa sin necesidad de responder a una solicitud de confirmación en su dispositivo ni de enviar una contraseña de un solo uso desde un identificador.
 6. Haga clic en **Guardar**. La duración se muestra en el resumen de usuario.
 7. De forma opcional, haga clic en **Cancelar** en el resumen de usuario para finalizar el periodo de autenticación previa. Los usuarios también pueden finalizar el periodo de autenticación previa haciendo clic en **Caducar ahora** en BlackBerry UEM Self-Service.

Pasos para administrar identificadores de hardware de contraseña de un solo uso

Para utilizar la función de identificadores de contraseña de un solo uso (OTP), puede llevar a cabo lo siguiente:

Paso	Acción
1	Activación de la función de identificadores de OTP.
2	Si es necesario, convierta un archivo de información de identificador de un archivo .xml en formato PSCK a un archivo .csv que pueda importar a BlackBerry UEM, Uso de la herramienta de conversión del identificador de BlackBerry 2FA . Para obtener más información, consulte Modificación del archivo de configuración CSVConfig .
3	Importación de identificadores de OTP en BlackBerry UEM
4	Asignación de un identificador de OTP a un usuario

Activación de la función de identificadores de OTP

1. En la barra de menú, haga clic en **Configuración > Integración externa > Identificadores de contraseña de un solo uso**.
2. Haga clic en **Activar**.
3. Haga clic en **Activar**.

Desactivación de la función de identificadores de OTP

1. En la barra de menú, haga clic en **Configuración > Integración externa > Identificadores de contraseña de un solo uso**.
2. Haga clic en **Desactivar gestión de identificadores de contraseñas de un solo uso**.
3. Si es necesario, elimine los identificadores de OTP de BlackBerry UEM. Para obtener más información, consulte [Eliminación de un identificador de OTP de BlackBerry UEM](#).

Identificadores de hardware de contraseña de un solo uso compatibles

BlackBerry 2FA actualmente es compatible con los siguientes identificadores de hardware de contraseña de un solo uso (OTP) de terceros:

- RCDevs RC200

- Vasco DIGIPASS GO 6
- Feitian OTP C200

Se incluirá una mayor compatibilidad con más identificadores de hardware en las siguientes versiones. Para obtener la última información sobre compatibilidad de los identificadores de hardware, consulte la [matriz de compatibilidad del servidor](#).

Uso de la herramienta de conversión del identificador de BlackBerry 2FA

Nota: Esta herramienta solo está disponible y es necesaria para BlackBerry UEM 12.7. Para BlackBerry UEM 12.8 y posteriores y BlackBerry UEM Cloud, los archivos de información de identificadores se pueden importar directamente en UEM sin utilizar la herramienta.

Utilice la herramienta de conversión del identificador de BlackBerry 2FA para convertir un archivo de información de identificador de un archivo .xml en formato PSCK a un archivo .csv que pueda importar a BlackBerry UEM. Cuando la conversión de un archivo se realiza con éxito, el archivo generado se guarda automáticamente en la misma carpeta que la herramienta.

Para los identificadores Vasco y Feitian, debe utilizar la herramienta de conversión del identificador de BlackBerry 2FA para convertir los archivos de información del identificador que el fabricante proporciona a un formato que BlackBerry UEM pueda leer.

La herramienta de conversión del identificador de BlackBerry 2FA solo es compatible con los archivos de información del identificador en formato PSKC (Portable Symmetric Key Container; contenedor de claves simétricas portátil). Para obtener más información acerca de PSKC, consulte <https://tools.ietf.org/html/rfc6030>.

Importante: El archivo generado contiene información del identificador sin cifrar. Se recomienda encarecidamente que solo ejecute la herramienta de conversión del identificador de BlackBerry 2FA en un entorno informático seguro y elimine el archivo generado inmediatamente después de importarlo a BlackBerry UEM.

Antes de empezar:

- Descargue la herramienta de conversión del identificador de BlackBerry 2FA en <https://swdownloads.blackberry.com/Downloads/entry.do?code=0C52D419A421FB13BB58357E67B7FB4B>.
- Coloque los archivos de información del identificador que desee convertir en la misma carpeta que la herramienta.

1. Abra la línea de comandos.
2. Examine el directorio de la herramienta de conversión del identificador de BlackBerry 2FA.
3. Ejecute **tokenConversionTool-<versión>.jar** con los siguientes parámetros:

Parámetro	Descripción
-h	Para mostrar el mensaje de uso de la ayuda.
-v	Opcionalmente, active el modo detallado. Si activa el modo detallado, la información del identificador del archivo especificado se muestra en la línea de comandos.

Parámetro	Descripción
-f	De manera opcional, especifique el formato que desea convertir a "basic" o "rcdevs". El valor predeterminado es "rcdevs".
-p	Si es necesario, especifique la clave del identificador necesaria para descifrar el archivo de información del identificador. La contraseña es una secuencia de bytes en formato hexadecimal (p. ej., A12BC34D).
<i>Nombre del archivo</i>	Especifique el archivo que desea convertir. El archivo debe estar en la misma carpeta que la herramienta. Este parámetro es necesario.

Por ejemplo, escriba uno de los siguientes:

- `java -jar <nombreHerramienta>.jar -f basic -p <contraseña> ./<nombreArchivoIdentificador>.xml`
- `java -jar tokenConversionTool-1.0.4.jar ./vasco.xml`

La ruta del archivo de salida aparece cuando el archivo se genera correctamente.

Después de terminar: Importe el archivo de información del identificador generado a la consola de gestión de BlackBerry UEM. Para obtener más información, consulte [Importación de identificadores de OTP en BlackBerry UEM](#).

Modificación del archivo de configuración CSVConfig

El archivo .csv que contiene los datos de los identificadores requiere un archivo de configuración (CSVConfig.json) que define la forma en que el archivo .csv es analizado por BlackBerry UEM. El archivo .csv debe analizarse correctamente antes de que los datos de los identificadores se extraigan y se importen en la base de datos de BlackBerry UEM.

La primera vez que inicie sesión en BlackBerry UEM tras activar la función de identificadores de OTP, se generará un archivo CSVConfig.json predeterminado. El archivo se genera con valores predeterminados y se guarda en "BESNG_HOME"/otp/config/CSVConfig.json (o C:\otp\config\CSVConfig.json).

La siguiente información le ayudará a modificar el archivo CSVConfig.json para asegurarse de que el archivo .csv es analizado correctamente por BlackBerry UEM.

- La configuración recomendada para la "extensión" es "CSV".
- La configuración recomendada para "stripSpacesAndQuotations" es "true". Todos los espacios y las comillas de las columnas se eliminan.
- Las columnas de cada campo de datos pueden tener un máximo de cuatro parámetros para determinar la manera en que BlackBerry UEM analizará y extraerá los datos de la columna correspondiente.
 - "column" determina el número de columna en el archivo .csv. Las columnas se inician en "0".
 - "startCharPos" determina dónde se inician los datos del identificador en la columna. Si "stripSpacesAndQuotations" se establece en "true", solo se tienen en cuenta los caracteres anteriores al inicio de los datos del identificador real, y no los espacios ni las comillas.

- "endCharPos" determina dónde finalizan los datos del identificador en la columna. Si "stripSpacesAndQuotations" se establece en "true", solo se tienen en cuenta los caracteres anteriores al fin de los datos del identificador real, y no los espacios ni las comillas.
- "encoding" determina la codificación o descodificación de caracteres utilizada. "base64" es estándar.

El siguiente es un ejemplo de un archivo CSVConfig.json actualizado para analizar un archivo .csv relleno con información de identificadores de RCDevs:

```
{
  "extension" : "CSV",
  "stripSpacesAndQuotations" : true,
  "startRow" : 4,
  "token_serial_number" : {
    "column" : 1,
    "startCharPos" : 0
  },
  "password_seed" : {
    "column" : 3,
    "startCharPos" : 9,
    "encoding" : "base64"
  },
  "password_length" : {
    "column" : 6,
    "startCharPos" : 10,
    "encoding" : "base64"
  },
  "time_step" : {
    "column" : 7,
    "startCharPos" : 13,
    "encoding" : "base64"
  },
  "vendor" : {
    "column" : 2,
    "startCharPos" : 0,
    "endCharPos" : 6
  },
  "model" : {
    "column" : 2,
    "startCharPos" : 6,
    "endCharPos" : 14
  },
  "t0" : {
    "column" : 5,
    "startCharPos" : 11,
    "encoding" : "base64"
  }
}
```

El siguiente es un ejemplo de texto sin formato de un archivo .csv relleno con información de identificadores de RCDevs.

```
1 # Inventory Import File for RCDevs WebADM
2 # Generated on June 29, 2016, 2:40 pm
3
4 Type                Reference                Description                Data
5 "OTP Token", "2308602200271", "RCDevs RC200-T6",
  "TokenKey=P6chCRszGaawHhpzWUHCS8Ua8WE=",TokenType=VE9UUA==,TokenState=MA==,OTPLength=Ng==,TO
6 "OTP Token", "2308602200272", "RCDevs RC200-T6",
  "TokenKey=Zghe8fbekGOXpwGM2vmEcZyZnaE=",TokenType=VE9UUA==,TokenState=MA==,OTPLength=Ng==,TO
```

```
7 "OTP Token", "2308602200273", "RCDevs RC200-T6",  
  "TokenKey=EH//86f6pnup3F4AS7w7HNazYjU=", TokenType=VE9UUA==, TokenState=MA==, OTPLength=Ng==, TO  
8 "OTP Token", "2308602200274", "RCDevs RC200-T6", "TokenKey=tzrVqKFMns9/  
rbAyCYCdDxb04Ig=", TokenType=VE9UUA==, TokenState=MA==, OTPLength=Ng==, TOTPTimeStep=MzA="
```

Importación de identificadores de OTP en BlackBerry UEM

Para importar identificadores de OTP, necesita un archivo .csv (delimitado por comas) que contenga información sobre los identificadores. El archivo.csv se lee con BlackBerry UEM utilizando un archivo de configuración (CSVConfig.json).

Antes de empezar: Debe modificar el archivo CSVConfig.json predeterminado para que BlackBerry UEM pueda analizar correctamente y almacenar a continuación la información de los identificadores en la base de datos. Para obtener más información, consulte [Modificación del archivo de configuración CSVConfig](#).

1. En la barra de menú, haga clic en **Configuración > Integración externa > Identificadores de contraseña de un solo uso**.
2. Haga clic en **Examinar**.
3. Desplácese hacia el archivo .csv que contiene la información sobre los identificadores y selecciónelo.
4. Haga clic en **Cargar**.

Eliminación de un identificador de OTP de BlackBerry UEM

1. En la barra de menú, haga clic en **Configuración > Integración externa > Identificadores de contraseña de un solo uso**.
2. Busque y seleccione el número de serie del identificador que desea eliminar.
3. Haga clic en  .
4. Haga clic en **Eliminar**.

Asignación de un identificador de OTP a un usuario

Antes de empezar: [Asignar un perfil de BlackBerry 2FA a un grupo](#).

1. En la barra de menú, haga clic en **Users**. Busque y seleccione el nombre del usuario.
2. En la página de detalles del usuario, haga clic en **Identificadores de contraseña de un solo uso**.
3. Busque y seleccione el número de serie del identificador que desea asignar al usuario.
4. Haga clic en **Asignar**.

Eliminación de un identificador de OTP de un usuario

1. En la barra de menú, haga clic en **Users**. Busque y seleccione el nombre del usuario.
2. En la página de detalles del usuario, haga clic en **Identificadores de contraseña de un solo uso**.
3. En **Identificadores asignados**, haga clic en **Eliminar**.

4. Haga clic en **Enviar** para anular la asignación del identificador de contraseña de un solo uso.

Adaptación automática de identificadores de hardware no sincronizados

Ahora se puede ajustar la ventana de frecuencia temporal de los identificadores de hardware para que se adapten automáticamente al desfase del identificador. Cuando el reloj interno del identificador de hardware se aleja demasiado de la hora correcta, el identificador muestra códigos no válidos. Si aumenta la ventana de frecuencia temporal, cualquier código dentro de dicha ventana será válido, aunque el identificador no esté sincronizado.

Por ejemplo, si establece la ventana de frecuencia temporal en "2", el código que se muestra en el identificador se aceptará como un código válido si precede o sigue el código previsto por dos intervalos de actualización. En este ejemplo, si el código que aparece en el identificador es el tercer código que precede o sigue al código previsto, el código no se considerará válido y la contraseña temporal se rechazará.

Este ajuste determina la ventana de frecuencia temporal para todos los identificadores de hardware. Ajuste la ventana de frecuencia temporal en función del número de intervalos de actualización en los que se considera que los identificadores han quedado desincronizados.

1. En la consola de gestión, haga clic en **Configuración > Integración externa**.
2. Haga clic en **Identificadores de contraseñas de un solo uso de BlackBerry 2FA**.
3. En el campo **Ventana de frecuencia temporal**, haga clic en .
4. Escriba un valor entre 0 y 50. El valor predeterminado es 3. Para aceptar solo el código previsto, que puede coincidir o no con el código que aparece en el identificador, establezca el valor de la ventana de frecuencia temporal en 0.
5. Haga clic en **Actualizar**.

Resincronización manual de un identificador de hardware

Si un identificador de hardware de contraseña de un solo uso asignado a un usuario no se puede utilizar debido a que no se ha adaptado automáticamente el desfase, puede intentar resincronizar manualmente el identificador. Para resincronizar manualmente un identificador con BlackBerry UEM, el usuario debe proporcionarle dos códigos consecutivos.

1. En la barra de menú, haga clic en **Users**. Busque y seleccione el nombre del usuario.
2. Haga clic en **Identificadores de contraseña de un solo uso**.
3. En la sección **Identificador asignado**, haga clic en **Volver a sincronizar**.
4. En el campo **Ventana de frecuencia temporal**, introduzca el número máximo de frecuencias temporales con las que desea sincronizar el identificador no sincronizado.
5. En el campo **Primer código de identificador**, introduzca el código que se muestra en el identificador.
6. En el campo **Segundo código de identificador**, introduzca el siguiente código consecutivo que se muestra en el identificador.
7. Haga clic en **Volver a sincronizar**.

Registros e informes

BlackBerry UEM genera registros para las funciones de autenticación previa y autorrescate de BlackBerry 2FA. Los registros se almacenan en el archivo de registro (CORE) de BlackBerry UEM Core.

Además de la información de registro para fines generales de resolución de problemas, BlackBerry UEM genera líneas especiales de registro para la actividad de autenticación previa y autorrescate, para fines de auditoría. Puede extraer estas líneas de registro para supervisar el uso global de las funciones de autenticación previa y autorrescate. Estas líneas de registro se registran en el nivel INFO, y constan de datos separados por comas y precedidas de información de registro CORE universal, que puede descartarse.

Estas líneas especiales de registro están etiquetadas con marcadores que le permiten extraerlas fácilmente. Se supervisan dos tipos de actividades: solicitudes de autenticación previa y solicitudes de autenticación de usuarios autenticados previamente. Cuando se extraen estas líneas y se descarta la información de registro CORE universal, puede abrir los datos separados por comas con cualquier software que admita el formato CSV. Para obtener más información acerca de registros e informes, consulte el [contenido de mantenimiento y supervisión de BlackBerry UEM](#).

Auditoría de solicitudes de autenticación previa

BlackBerry UEM registra todas las solicitudes de autenticación previa de BlackBerry 2FA y todas las solicitudes de autenticación durante la autenticación previa. Los datos se registran cuando la solicitud se completa o caduca.

El archivo de registro de auditoría incluye la siguiente información sobre todas las solicitudes de autenticación previa:

- Marcador1: BB2FA_AUDIT. Este es el identificador de todas las líneas de registro de auditoría de BlackBerry 2FA en el registro BlackBerry UEM Core. También indica dónde cortar las líneas de registro para descartar la información de registro CORE universal.
- Marcador2: PREAUTH_REQUEST. Este es el identificador del tipo de evento (solicitud de autenticación previa).
- Fecha
- Hora
- Fuente: consola de administración de BlackBerry UEM, BlackBerry UEM Self-Service, dispositivo del usuario
- Nombre de usuario
- Nombre del perfil de BlackBerry 2FA: el nombre se registra entre comillas para evitar que el campo se divida mediante comas en el perfil.
- Duración de la autenticación previa solicitada en horas
- Duración máxima configurada de la autenticación previa en horas
- Resultado: SUCCESS (éxito), FAILED_INVALID_REQUEST (error, solicitud no válida)
- Hora de caducidad de la autenticación previa

Por ejemplo:

```
2BB2FA_AUDIT,PREAUTH_REQUEST,2016-11-05,13:27:17.822,admin,user1,"Sales BB2FA Profile",3,12,May 11 16:41
```

El archivo de registro de auditoría incluye la siguiente información sobre todas las solicitudes de autenticación durante la autenticación previa:

- Marcador1: BB2FA_AUDIT. Este es el identificador de todas las líneas de registro de auditoría de BlackBerry 2FA en el registro BlackBerry UEM Core. También indica dónde cortar las líneas de registro para descartar la información de registro CORE universal.

- Marcador2: AUTH_USER_IN_PREAUTH. Este es el identificador del tipo de evento (solicitud de autenticación durante la autenticación previa).
- Fecha
- Hora
- ID de transacción
- Fuente: aplicación BlackBerry 2FA, BlackBerry Enterprise Identity, etc.
- Nombre de usuario
- Política de autenticación: contraseña de empresa, contraseña del dispositivo activa, contraseña del dispositivo pasiva
- Nombre del perfil: el nombre se registra entre comillas para evitar que el campo se divida mediante comas en el perfil.
- Hora de caducidad de la autenticación previa

Por ejemplo:

```
BB2FA_AUDIT,AUTH_USER_IN_PREAUTH,2016-11-05,13:27:17.822,50dbelcc,BB2FA,user1,Enterprise Password,"Sales BB2FA Profile",May 11 16:41
```

Aviso legal

© 2018 BlackBerry Limited. BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, MOVIRTU y SECUSMART, entre otras, son marcas comerciales o marcas registradas de BlackBerry Limited, de sus subsidiarias o filiales, sujetas a licencia, cuyos derechos exclusivos están expresamente reservados. El resto de marcas comerciales pertenecen a sus respectivos propietarios.

Android es una marca comercial de Google Inc. iOS es una marca comercial de Cisco Systems, Inc. o de sus filiales en EE. UU. y otros países. iOS® se usa bajo licencia de Apple Inc. Microsoft y Windows son marcas comerciales registradas o marcas comerciales de Microsoft Corporation en Estados Unidos y/o en otros países. El resto de marcas comerciales pertenecen a sus respectivos propietarios.

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, COMERCIALIZACIÓN, 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, EXTRA CONTRACTUAL O CUALQUIER OTRA, INCLUIDA CUALQUIER RESPONSABILIDAD POR NEGLIGENCIA O RESPONSABILIDAD ESTRICTA.

LAS LIMITACIONES, EXCLUSIONES Y DESCARGOS DE RESPONSABILIDAD SE APLICARÁN: (A) INDEPENDIEMENTE 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
200 Bath Road
Slough, Berkshire SL1 3XE
Reino Unido

Publicado en Canadá