BlackBerry 2FA

guía de configuración del servidor

3.2

Contents

Pasos para configurar el servidor de BlackBerry 2FA

Al configurar el servidor de BlackBerry 2FA, realice las siguientes acciones.

Tarea	Descripción
1	Si es necesario, descargue e instale el servidor de BlackBerry 2FA. Después de instalar el servidor, debe generar y descargar un archivo de activación y utilizarlo para permitir la comunicación entre el servidor de BlackBerry 2FA y BlackBerry UEM. Para obtener más información, consulte la guía de instalación y actualización del servidor de BlackBerry 2FA.
2	En el servidor VPN, cree un perfil para el servidor de BlackBerry 2FA. Para obtener más información, consulte Configuración de una conexión entre el servidor de BlackBerry 2FA y una puerta de enlace VPN.
3	Configuración del servidor de BlackBerry 2FA para que se conecte a una puerta de enlace VPN
4	Configuración de la conexión al extremo de la API de REST
5	Creación de un cliente API de REST en el servidor de BlackBerry 2FA
6	Activación de la autenticación MS-CHAP para usuarios en un dominio
7	Configuración de la aplicación BlackBerry 2FA
8	Asignación de puerta de enlace VPN o configuraciones de cliente de REST a un grupo de usuarios
9	Si es necesario, envíe la aplicación BlackBerry 2FA a los dispositivos. Para obtener más información, consulte Instalación de la aplicación BlackBerry 2FA en dispositivos.

Configuración de una conexión entre el servidor de BlackBerry 2FA y una puerta de enlace VPN

En su servidor VPN, el servidor de BlackBerry 2FA debe configurarse como un servidor RADIUS al que se envíen las solicitudes de autenticación. El servidor de BlackBerry 2FA completa las siguientes tareas para autenticar usuarios de forma que puedan conectarse a una puerta de enlace VPN:

- Autentica el dispositivo del usuario o una contraseña de un solo uso (OTP)
- Actúa como un proxy para la autenticación de contraseña
- Combina los dos resultados para determinar si la autenticación fue correcta

También debe configurar un perfil de cliente VPN o cliente que permita a los usuarios seleccionar BlackBerry 2FA cuando inicien sesión en la VPN desde sus ordenadores.

Para cada servidor de BlackBerry 2FA de su entorno, el servidor RADIUS debe tener las siguientes opciones:

- Dirección IP o FQDN del ordenador que aloja el servidor de BlackBerry 2FA
- Tiempo de espera de entre 60 y 90 segundos para la conexión entre el servidor VPN y el servidor de BlackBerry 2FA
- Secreto compartido único
- Puerto de autenticación establecido en 1812
- En función de las opciones de autenticación disponibles, elija entre PAP, MS-CHAP v1, MS-CHAP v2 o EAP-MSCHAP

El perfil de cliente VPN debe tener el tiempo de espera establecido entre 30 y 60 segundos para la conexión entre el cliente VPN en los ordenadores del usuario y el servidor VPN.

Para obtener instrucciones sobre cómo configurar un servidor RADIUS o un perfil de cliente VPN, consulte la documentación para el servidor VPN que está utilizando.

Para obtener una lista de servidores VPN compatibles, consulte la la matriz de compatibilidad del servidor de BlackBerry 2FA.

Protocolos de autenticación compatibles para cada opción de autenticación

La siguiente tabla muestra los protocolos de autenticación que están disponibles para cada opción de autenticación que admite BlackBerry 2FA.

Nota: Si los usuarios se están autenticando con un identificador de contraseña de un solo uso (OTP), el servidor VPN debe estar configurado para autenticarlos mediante PAP. Las OTP no son compatibles con MSCHAPv1, MSCHAPv2 ni EAP-MSCHAP.

Opción de autenticación	Protocolos de autenticación compatibles
Autenticación de dos factores mediante contraseña de dispositivo pasiva	PAP
Autenticación de dos factores mediante contraseña de dispositivo activa	PAP

Opción de autenticación	Protocolos de autenticación compatibles
Autenticación de dos factores mediante contraseña de empresa	MS-CHAP v1, MS-CHAP v2, PAP y EAP-MSCHAP
Autenticación de factor único mediante contraseña de empresa	MS-CHAP v1, MS-CHAP v2, PAP y EAP-MSCHAP

Configuración de la conexión con el servidor de BlackBerry 2FA en una puerta de enlace VPN de Cisco ASA Series

Si está utilizando una puerta de enlace VPN Cisco ASA Series, puede crear un perfil VPN mediante la siguiente información.

Para obtener instrucciones detalladas sobre cómo configurar el perfil VPN, visite http://www.cisco.com para leer la documentación de Cisco ASA Series.

Al crear el perfil, debe establecer las siguientes opciones para admitir BlackBerry 2FA:

- Para cada servidor de BlackBerry 2FA de su entorno, cree un grupo de servidores RADIUS AAA con las siguientes opciones:
  - Dirección IP o FQDN del ordenador que aloja el servidor de BlackBerry 2FA
  - Tiempo de espera de entre 60 y 90 segundos para establecer la conexión entre la puerta de enlace VPN y el servidor de BlackBerry 2FA
  - Secreto compartido único
  - Puerto de autenticación establecido en 1812
  - Compatible con MS-CHAP v2
- Para la conexión entre el cliente VPN de los ordenadores del usuario y la puerta de enlace VPN, establezca el tiempo de espera en entre 30 y 60 segundos. Debe configurar el tiempo de espera en el archivo del perfil de cliente VPN de Cisco AnyConnect (un archivo XML) que debe instalarse en los ordenadores del usuario.
- Opción de gestión de contraseñas: si configura el perfil para que sea compatible con la autenticación de MS-CHAP v2

Debe completar las siguientes acciones para terminar el proceso de creación del perfil:

- Active el protocolo de encapsulamiento de carga de túnel de VPN (por ejemplo, el protocolo IPSEC IKE v2)
- Todos los comandos que son necesarios para el grupo de políticas de VPN asociado
- Todos los comandos que son necesarios para el perfil de cliente VPN asociado de Cisco AnyConnect y la creación del archivo XML en sí
- Todos los comandos que son necesarios para el grupo de túnel de VPN asociado

No necesita configurar la autenticación de certificado adicional.

Cuando configure la conectividad de la puerta de enlace VPN en el servidor BlackBerry 2FA, debe proporcionar el secreto compartido de RADIUS que ha creado en el perfil VPN.

Configuración de la conexión con el servidor de BlackBerry 2FA en Citrix NetScaler

Si está utilizando Citrix NetScaler, puede configurar la conexión con el servidor de BlackBerry 2FA añadiéndola como servidor RADIUS. Si tiene más de un servidor de BlackBerry 2FA en su entorno, debe configurar un servidor RADIUS independiente para cada uno de ellos.

Para obtener instrucciones detalladas sobre cómo configurar NetScaler con el fin de conectarse al servidor de BlackBerry 2FA, visite http://docs.citrix.com/en-us/netscaler.html para leer información sobre la configuración de la autenticación RADIUS en la documentación del sistema NetScaler.

Por ejemplo, puede configurar una conexión con un servidor de BlackBerry 2FA y utilizar BlackBerry 2FA como método de autenticación predeterminado. Si desea configurar este ejemplo, en la utilidad de configuración de NetScaler, debe configurar los valores de autenticación en la configuración global de la siguiente manera:

- "Número máximo de usuarios", "Intentos de inicio de sesión máximos" y "Error en el tiempo de espera de inicio de sesión", como lo requiera su empresa
- Tipo de autenticación establecido en RADIUS
- Dirección IP establecida en el servidor de BlackBerry 2FA
- Puerto establecido en 1812
- Tiempo de espera de entre 60 y 90 segundos para la conexión entre NetScaler y el servidor de BlackBerry 2FA
- Secreto compartido único
- "Activar extracción de dirección IP de NAS" seleccionada
- "Codificación de contraseña" establecida en el protocolo de autenticación compatible con la opción de autenticación VPN que ha elegido (BlackBerry 2FA no es compatible con la opción "chap")
- Contabilidad desactivada

Configuración de la conexión con el servidor de BlackBerry 2FA en F5BIG-IP

Si utiliza F5BIG-IP con un servidor AAA, puede crear una política de acceso con el administrador de la política de acceso utilizando la siguiente información.

Para obtener instrucciones detalladas sobre cómo configurar la autenticación mediante servidores AAA, visite https://support.f5.com/kb/en-us/products/big-ip_apm/manuals/product/apm_config_10_2_0/apm_config_server_auth.html para leer la documentación de F5BIG-IP.

Al crear la política, debe establecer las siguientes opciones para admitir BlackBerry 2FA:

- Que establezca el tipo de autenticación para RADIUS
- Que especifique la dirección IP o FQDN del ordenador que aloja el servidor de BlackBerry 2FA
- Que configure un tiempo de espera de entre 60 y 90 segundos para la conexión entre la puerta de enlace VPN y el servidor de BlackBerry 2FA
- Que establezca un secreto compartido único
- Que establezca el puerto de autenticación en 1812
- Que compruebe que MS-CHAP v2 es compatible
- Que desactive las cuentas
- Que especifique el número máximo de intentos de inicio de sesión

La política debe asignarse a cada servidor de BlackBerry 2FA de su entorno.

Configuración de la conexión al servidor de BlackBerry 2FA en Barracuda SSL VPN

Si está utilizando Barracuda SSL VPN, puede configurar la conexión con el servidor de BlackBerry 2FA añadiéndola como servidor RADIUS. Si tiene más de un servidor de BlackBerry 2FA en su entorno, debe configurar un servidor RADIUS independiente para cada uno de ellos.

Para obtener instrucciones detalladas sobre cómo configurar Barracuda SSL VPN para conectarse al servidor de BlackBerry 2FA, visite https://www.barracuda.com/support/knowledgebase/50160000000HZG9AAO.

Debe configurar un servidor RADIUS con las siguientes opciones para admitir BlackBerry 2FA:

- Que establezca el tipo de autenticación para RADIUS
- Que especifique la dirección IP o FQDN del ordenador que aloja el servidor de BlackBerry 2FA
- Que configure un tiempo de espera de entre 60 y 90 segundos para la conexión entre la puerta de enlace VPN y el servidor de BlackBerry 2FA
- Que establezca un secreto compartido único
- Que establezca el puerto de autenticación en 1812
- Que compruebe que MS-CHAP v2 es compatible
- Que desactive las cuentas
- Que especifique el número máximo de intentos de inicio de sesión

Configuración de la conexión al servidor de BlackBerry 2FA en un servidor strongSwan

Para configurar la conectividad al servidor de BlackBerry 2FA en un servidor strongSwan, debe modificar los archivos ipsec.conf y eap-radius.conf.

Para obtener más información sobre estos archivos y sobre cómo configurar strongSwan, visite https://www.strongswan.org/.

Configuración de ipsec.conf

El archivo ipsec.conf está ubicado en el directorio /etc. Debe añadir una nueva sección "conn" al servidor de BlackBerry 2FA. Por ejemplo:

```
conn <nombre>
 keyexchange=ikev2
 rightauth=eap-radius
 rightsendcert=never
 eap_identity=%any
 auto=add
```

Configuración	Descripción
<name>	Este es el nombre único de la nueva sección de conexión. Es habitual que el nombre refleje algunas características clave de la propia conexión (por ejemplo, IPSec-IKEv2-radius).

Configuración	Descripción
keyexchange=ikev2	Esta configuración especifica el método de intercambio de claves (por ejemplo, IKEv1, IKEv2). El servidor de BlackBerry 2FA no utiliza esta configuración, pero debe incluirla en la sección conn para activar el intercambio de claves correcto con clientes VPN. Debe asegurarse de que los clientes VPN que se conecten al servidor strongSwan utilicen el mismo método de intercambio de claves.
rightauth=eap-radius	Esta configuración especifica que el servidor strongSwan debe utilizar EAP a través de RADIUS para autenticar a los clientes VPN para este tipo de conexión.
rightsendcert=never	Esta configuración especifica que los certificados de usuario no se utilizan para la autenticación de clientes.
eap_identity=%any	Esta configuración especifica la identidad del cliente VPN que se utilizará para la autenticación. El servidor de BlackBerry 2FA no utiliza esta configuración, pero debe incluirla en la sección conn. El valor "%any" indica al servidor strongSwan que pase la identidad proporcionada por el cliente VPN.
auto=add	Esta configuración especifica que esta sección de conexión está activa. El servidor de BlackBerry 2FA no utiliza esta configuración, pero debe incluirla en la sección conn.

Configuración eap-radius.conf

El archivo eap-radius.conf está ubicado en el directorio /etc/strongswan.d/charon. Especifica los detalles de la autenticación de EAP a través de RADIUS. El archivo de configuración predeterminado tiene todas las configuraciones que debe configurar, pero la mayoría están comentados y algunos no tienen ningún valor asignado. Debe modificar la configuración necesaria eliminando el signo de almohadilla (#) y estableciendo los valores como se describe en la siguiente tabla.

Configuración	Descripción
accounting=no	Esta configuración evita que strongSwan envíe información de cuentas RADIUS al servidor de BlackBerry 2FA.
nas_identifier	Esta configuración opcional especifica el identificador de NAS que debe incluirse en los mensajes RADIUS. Puede utilizar esta configuración si varios servidores strongSwan están utilizando el mismo servidor de BlackBerry 2FA.
port=1812	Esta configuración especifica el puerto utilizado por el servidor de BlackBerry 2FA para recibir solicitudes RADIUS para la autenticación.
secret=<*secreto compartido*>	Esta configuración especifica el secreto compartido entre strongSwan y el servidor de BlackBerry 2FA. Al configurar la conectividad del servidor VPN en el servidor de BlackBerry 2FA, debe escribir el secreto compartido RADIUS que especifique aquí.

Configuración	Descripción
server=<*IP del servidor VPNAuth*>	Esta configuración especifica la dirección IP o el FQDN del servidor de BlackBerry 2FA.
ike_to_radius=1, 2, 311:1, 311:11, 311:25	Esta configuración especifica una lista de números separada por comas que representa la lista de atributos RADIUS que necesita strongSwan para reenviar al servidor de BlackBerry 2FA. Los números separados por dos puntos indican atributos específicos del proveedor. El primer número identifica al proveedor (por ejemplo, 311 es el número de Microsoft) y el segundo número identifica el tipo de atributo. Esta configuración se encuentra en la sección "reenviar" del archivo de configuración.
radius_to_ike=311:26, 311:17, 311:16	Esta configuración especifica una lista de números separados por comas que representa la lista de atributos RADIUS que necesita el servidor de BlackBerry 2FA para reenviar a strongSwan. Los números separados por dos puntos indican atributos específicos del proveedor. El primer número identifica al proveedor (por ejemplo, 311 es el número de Microsoft) y el segundo número identifica el tipo de atributo. Esta configuración se encuentra en la sección "reenviar" del archivo de configuración.

Configuración del servidor de BlackBerry 2FA para que se conecte a una puerta de enlace VPN

Antes de empezar: Obtenga la dirección IP y el secreto compartido de las puertas de enlace VPN.

1. En la barra de menú de la consola de administración de BlackBerry UEM, haga clic en **Configuración** > **Integración externa** > **Servidor de BlackBerry 2FA**.
2. Haga clic en el servidor de BlackBerry 2FA que desee para configurar una puerta de enlace VPN.
3. En la sección **Configuración de VPN**, haga clic en +.
4. En el campo **Nombre del servidor VPN**, escriba un nombre único para la puerta de enlace VPN a la que se está conectando.
5. En el campo **Host VPN**, escriba la dirección IP de la puerta de enlace VPN.
6. En los campos **Secreto compartido** y **Confirmar secreto compartido**, escriba y confirme el secreto compartido de la puerta de enlace VPN.
7. De forma opcional, anule la configuración de la aplicación BlackBerry 2FA. Puede configurar los siguientes campos independientes entre sí. Los campos vacíos se ignoran y se utilizan los valores predeterminados de la sección **Aviso predeterminado del dispositivo**.
   a) Seleccione **Aviso de BlackBerry 2FA para esta VPN**.
   b) En el campo **Título**, escriba el título que desee que muestre la aplicación en su mensaje. Por ejemplo, "VPN de la empresa de ejemplo".

c) En el campo **Mensaje**, escriba el mensaje que desee que muestre la aplicación a los usuarios. Este mensaje explica a los usuarios qué se requiere de ellos.
d) En el campo **Confirmar texto del botón**, escriba el texto que aparece en el botón que pueden tocar los usuarios para confirmar la autenticación de segundo factor.
e) En el campo **Rechazar texto del botón**, escriba el texto que aparece en el botón que pueden tocar los usuarios para rechazar la autenticación de segundo factor.
f) En el tiempo de espera **Tiempo de espera (segundos)**, escriba la cantidad de tiempo, en segundos, antes de que caduque la transacción de autenticación.

8. Haga clic en **Agregar**.
9. Repita estos pasos para cada puerta de enlace VPN que desee agregar.
10. Haga clic en **Guardar**.

Actualización de una conexión a una puerta de enlace VPN

1. En la barra de menú de la consola de administración de BlackBerry UEM, haga clic en **Configuración** > **Integración externa** > **Servidor de BlackBerry 2FA**.
2. Haga clic en el nombre del servidor de 2FA que desee configurar.
3. Haga clic en el nombre del servidor VPN que desee actualizar.
4. Actualice la configuración según sea necesario. Para obtener más información, consulte los pasos del 4 al 7 de Configuración del servidor de BlackBerry 2FA para que se conecte a una puerta de enlace VPN.
5. Haga clic en **Agregar**.
6. Haga clic en **Guardar**.

Eliminación de una conexión a una puerta de enlace VPN

1. En la barra de menú de la consola de administración de BlackBerry UEM, haga clic en **Configuración** > **Integración externa** > **Servidor de BlackBerry 2FA**.
2. Junto al servidor VPN que desea eliminar, haga clic en ✕.
3. Haga clic en **Sí**.
4. Haga clic en **Guardar**.

Configuración de la conexión al extremo de la API de REST

El extremo de la API de REST del servidor de BlackBerry 2FA se protege mediante un HTTPS autenticado en servidor. Debe configurar sus servicios personalizados para confiar en el servidor de BlackBerry 2FA. Tiene las siguientes opciones:

- Puede utilizar el certificado autofirmado predeterminado que se genera durante la instalación del servidor de BlackBerry 2FA. El certificado autofirmado predeterminado se encuentra en bb2fa-config/restkeystore.jks. Su aplicación cliente debe estar configurada para confiar en este certificado de forma explícita. El puerto del servidor predeterminado es el 5443.
- Puede proporcionar su propio certificado firmado por una CA importándolo en un almacén de claves Java con el alias "bb2fa" (se recomienda RSA 2048 como algoritmo de clave). Copie el archivo del almacén de claves en el directorio bb2fa-config y actualice el nombre de archivo del almacén de claves y la contraseña en la página de configuración del servidor de BlackBerry 2FA en BlackBerry UEM.

En todos los casos, los servicios personalizados se autentican mediante autenticación básica HTTP (nombre de usuario y contraseña) que se envían como encabezados en la solicitud.

1. En la barra de menú de la consola de administración de BlackBerry UEM, haga clic en **Configuración** > **Integración externa** > **Servidor de BlackBerry 2FA**.
2. Haga clic en el nombre del servidor de 2FA que desee configurar.
3. En la sección **Configuración de la interfaz de REST**, introduzca la información.
4. Haga clic en **Guardar**.

Configuración de la conectividad del extremo de la API de REST

Para configurar la conectividad entre aplicaciones cliente y el extremo de la API de REST del servidor de BlackBerry 2FA, debe configurar sus aplicaciones cliente para confiar en el servidor de BlackBerry 2FA.

Las aplicaciones cliente se autentican mediante autenticación básica HTTP (nombre de usuario y contraseña) que se envían como encabezados en la solicitud. El extremo de la API de REST se protege mediante HTTPS autenticada por el usuario (https://<*nombrehost*>:<*puerto*>/<*prefijo*>/). El puerto predeterminado es 5443 y el prefijo predeterminado es "rest". Las siguientes solicitudes de REST son compatibles con el extremo:

Ruta	Tipo	Descripción	Notas
/<*prefijo*>/ twofactor	POST	Solicitud de autenticación en dos fases	

El mensaje de solicitud se envía mediante HTTP POST y se le da formato JSON, con los siguientes parámetros:

Parámetro	Tipo	Descripción	Notas
nombre de usuario	Cadena	Nombre de usuario	
contraseña	Cadena	Contraseña de usuario o contraseña de un solo uso y contraseña de usuario	Opcional, según la política

Parámetro	Tipo	Descripción	Notas
política	Valor entero	Opción de autenticación: • 0: autenticación de factor único mediante contraseña de empresa • 1: autenticación de dos factores con contraseña de empresa • 2: autenticación de dos factores con contraseña de dispositivo activa • 3: autenticación de dos factores con contraseña de dispositivo pasiva	
oneTimePassword	Cadena	Contraseña de un solo uso	Opcional
messageTitle	Cadena	Cuadro de diálogo del texto del título	Opcional
mensaje	Cadena	Cuadro de diálogo del texto del mensaje	Opcional
confirmButtonText	Cadena	Cuadro de diálogo de texto del botón de confirmar	Opcional
declineButtonText	Cadena	Cuadro de diálogo de texto del botón de rechazar	Opcional
tiempo de espera	Valor entero	Cuadro de diálogo de tiempo de espera (segundos)	Opcional

El cuerpo del mensaje de respuesta tiene formato JSON, con el siguiente parámetro:

Parámetro	Tipo	Descripción	Notas
información	Cadena	Mensaje informativo	

El mensaje de respuesta también incluye los siguientes códigos de estado HTTP:

Estado	Descripción	Notas
200	Aceptar	Autenticación correcta
400	Solicitud incorrecta	Parámetros no válidos
401	Sin autorización	La autenticación ha fallado
403	Declinada	Autenticación rechazada por el usuario

Estado	Descripción	Notas
500	Error interno de servidor	Error interno

Creación de un cliente API de REST en el servidor de BlackBerry 2FA

1. En la barra de menú de la consola de administración de BlackBerry UEM, haga clic en **Configuración** > **Integración externa** > **Servidor de BlackBerry 2FA**.
2. Haga clic en el nombre del servidor de 2FA que desee configurar.
3. En la sección **Configuración del cliente de REST**, haga clic en +.
4. En el campo **Nombre del cliente de REST**, escriba un nombre descriptivo para el cliente.
5. En el campo **ID del cliente de REST**, escriba un nombre para el cliente que se asociará con la contraseña.
6. En el campo **Contraseña**, escriba una contraseña. La contraseña debe tener un mínimo de ocho caracteres
7. En el campo **Confirmar contraseña**, vuelva a escribir la contraseña.
8. Haga clic en **Agregar**.
9. Repita estos pasos para cada cliente que desee agregar.
10. Haga clic en **Guardar**.

Activación de la autenticación MS-CHAP para usuarios en un dominio

Puede activar un servidor de BlackBerry 2FA con el fin de admitir la autenticación MS-CHAPv1 y MS-CHAPv2 para las solicitudes RADIUS (por ejemplo, las procedentes de una puerta de enlace VPN) para los usuarios que sean miembros del dominio seleccionado. El dominio está disponible para esta opción, ya que el servidor de 2FA funciona en un host combinado con un dominio Active Directory al que BlackBerry UEM también está conectado.

1. En la barra de menú de la consola de administración de BlackBerry UEM, haga clic en **Configuración** > **Integración externa** > **Servidor de BlackBerry 2FA**.
2. Haga clic en el nombre del servidor de 2FA que desee configurar.
3. En la sección **Configuración de Active Directory**, seleccione el dominio para el que quiere activar la autenticación MS-CHAP. Para desactivar la autenticación MS-CHAP, anule la selección del dominio.
4. Haga clic en **Guardar**.

Configuración de la aplicación BlackBerry 2FA

Puede personalizar el mensaje predeterminado que BlackBerry 2FA muestra a los usuarios cuando se conectan a los recursos que ofrece. También puede establecer la cantidad de tiempo, en segundos, antes de que caduque la solicitud de autenticación.

También puede anular esta configuración para cada puerta de enlace VPN que configure. Para obtener más información acerca de la configuración de puertas de enlace VPN, consulte Configuración del servidor de BlackBerry 2FA para que se conecte a una puerta de enlace VPN.

1. En la barra de menú de la consola de administración de BlackBerry UEM, haga clic en **Configuración** > **Integración externa** > **Servidor de BlackBerry 2FA**.
2. Haga clic en el nombre del servidor de 2FA que desee configurar.
3. En la sección **Aviso predeterminado del dispositivo**, lleve a cabo los pasos siguientes:
   a) En el campo **Título**, escriba el título que desee que muestre la aplicación en su mensaje. Por ejemplo, "VPN de la empresa de ejemplo".
   b) En el campo **Mensaje**, escriba el mensaje que desee que muestre la aplicación a los usuarios. Este mensaje explica a los usuarios qué se requiere de ellos.
   c) En el campo **Confirmar texto del botón**, escriba el texto que aparece en el botón que pueden tocar los usuarios para confirmar la autenticación de segundo factor.
   d) En el campo **Rechazar texto del botón**, escriba el texto que aparece en el botón que pueden tocar los usuarios para rechazar la autenticación de segundo factor.
   e) En el tiempo de espera **Tiempo de espera (segundos)**, escriba la cantidad de tiempo, en segundos, antes de que caduque la transacción de autenticación.
4. Haga clic en **Guardar**.

Asignación de puerta de enlace VPN o configuraciones de cliente de REST a un grupo de usuarios

Para autorizar el uso de VPN o clientes de REST a los usuarios, debe asignar una puerta de enlace VPN o una configuración de cliente de REST a los grupos de usuarios. Puede crear grupos de usuarios con aquellos usuarios a los que desea asignar las configuraciones. Los usuarios solo pueden utilizar las configuraciones que les asignan.

Antes de empezar: Lleve a cabo una de estas acciones:

- Configuración del servidor de BlackBerry 2FA para que se conecte a una puerta de enlace VPN
- Creación de un cliente API de REST en el servidor de BlackBerry 2FA

1. En la consola de administración de BlackBerry UEM, en la barra de menús, haga clic en **Grupos** > **Usuario**.
2. Puede crear un nuevo grupo o hacer clic en el nombre del grupo al que desea asignar una configuración.
3. Haga clic en la pestaña **BlackBerry 2FA**.
4. Haga clic en +.
5. Elija una configuración de cliente del dispositivo de la lista desplegable.
6. Haga clic en **Asignar**.

Instalación de la aplicación BlackBerry 2FA en dispositivos

BlackBerry 2FA está disponible para iOS, Android y dispositivos con BlackBerry 10.

Dispositivos iOS y Android

En los dispositivos con iOS y Android, se incluyen las funciones de BlackBerry 2FA en la aplicación BlackBerry UEM Client. Los usuarios deben descargarse BlackBerry UEM Client para activar su dispositivo con BlackBerry UEM para utilizar 2FA.

Los usuarios pueden descargar la aplicación BlackBerry UEM Client desde Google Play y la App Store.

Dispositivos BlackBerry 10

Para dispositivos con BlackBerry 10, debe enviar la aplicación BlackBerry 2FA a los dispositivos mediante BlackBerry UEM. Realice las siguientes acciones utilizando BlackBerry UEM:

- Si es necesario, utilice la consola de gestión de BlackBerry UEM para especificar una ubicación de red compartida para aplicaciones internas.
- En la consola de gestión de BlackBerry UEM, agregue el archivo de la aplicación BlackBerry 2FA (.bar) como aplicación interna. La aplicación BlackBerry 2FA está ubicada en: https://swdownloads.blackberry.com/Downloads/entry.do?code=0C52D419A421FB13BB58357E67B7FB4B
- En la consola de gestión de BlackBerry UEM, asigne la aplicación a las cuentas de usuario o grupos.

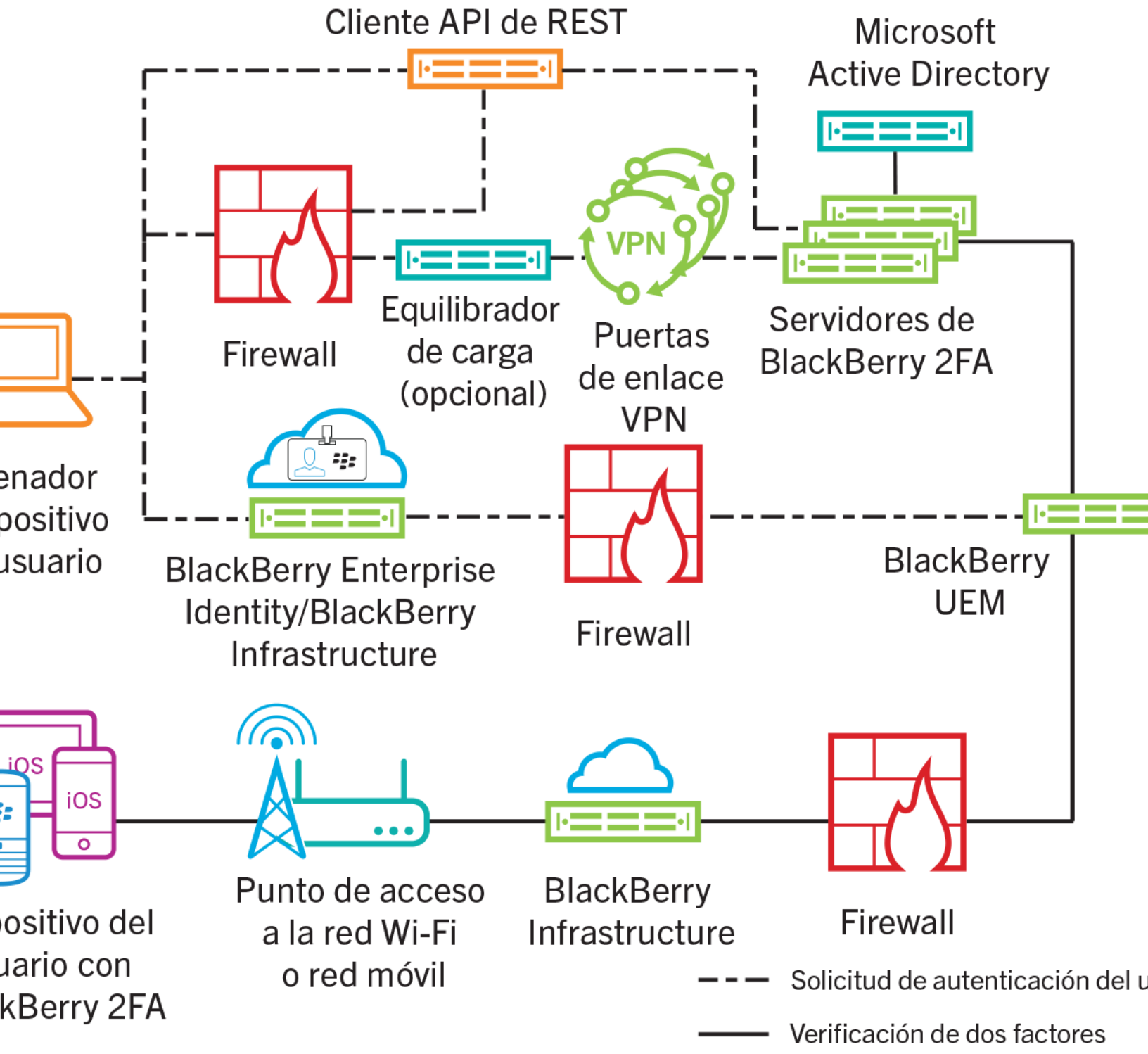
En el caso de dispositivos con un espacio de trabajo, la aplicación se instala en el espacio de trabajo. Los usuarios también pueden instalarla utilizando BlackBerry World para el trabajo si no hace obligatoria la instalación.

Para obtener más información sobre el envío de aplicaciones, consulte el contenido de administración de BlackBerry UEM.

Arquitectura: alta disponibilidad de BlackBerry 2FA

BlackBerry 2FA es compatible con la alta disponibilidad activo-activo. Puede instalar varias instancias del servidor de BlackBerry 2FA para proporcionar equilibrio de carga en las solicitudes de autenticación y promover la fiabilidad.

El siguiente diagrama muestra una situación de alta disponibilidad. Es posible que algunas soluciones VPN incluyan un equilibrador de carga y en esa situación no se requiere un equilibrador de carga independiente.


Cliente API de REST
Microsoft Active Directory
Firewall
Equilibrador de carga (opcional)
VPN
Puertas de enlace VPN
Servidores de BlackBerry 2FA
enador positivo usuario
BlackBerry Enterprise Identity/BlackBerry Infrastructure
Firewall
BlackBerry UEM
iOS
iOS
positivo del uario con kBerry 2FA
Punto de acceso a la red Wi-Fi o red móvil
BlackBerry Infrastructure
Firewall
Solicitud de autenticación del u
Verificación de dos factores

Configuración del servidor de BlackBerry 2FA para la alta disponibilidad

Puede utilizar los mismos puertos para todos los servidores de BlackBerry 2FA.

Para mantener el cifrado único de información de configuración, se recomienda que no copie el archivo bb2fa-config.json entre los servidores de BlackBerry 2FA. Debe configurar cada servidor por separado en la consola de gestión de BlackBerry UEM.

Tarea	Descripción
1	Si aún no lo ha hecho, configure la alta disponibilidad para la puerta de enlace VPN. Para obtener más información, consulte la documentación de la puerta de enlace VPN.
2	Instale dos o más servidores de BlackBerry 2FA. En cada servidor, genere y descargue un archivo de activación. Durante las subsiguientes instalaciones, puede elegir no seleccionar los archivos de la aplicación BlackBerry 2FA. No es necesario que instale los archivos más de una vez. Para obtener más información, consulte la guía de instalación y actualización del servidor de BlackBerry 2FA.
3	Cree un perfil para los servidores de BlackBerry 2FA en el servidor VPN. Para obtener más información, consulte Configuración de una conexión entre el servidor de BlackBerry 2FA y una puerta de enlace VPN.
4	Conecte cada servidor de BlackBerry 2FA a una puerta de enlace VPN. Para obtener más información, consulte Configuración del servidor de BlackBerry 2FA para que se conecte a una puerta de enlace VPN.
5	Configuración de la conexión al extremo de la API de REST
6	Creación de un cliente API de REST en el servidor de BlackBerry 2FA.
7	Activación de la autenticación MS-CHAP para usuarios en un dominio
8	Configuración de la aplicación BlackBerry 2FA
9	Asignación de puerta de enlace VPN o configuraciones de cliente de REST a un grupo de usuarioss
10	Si es necesario, envíe la aplicación BlackBerry 2FA a los dispositivos. Para obtener más información, consulte Instalación de la aplicación BlackBerry 2FA en dispositivos.

Registros e informes

BlackBerry 2FA almacena sus archivos de registro en *<directorio_instalación>*\logs. Hay cuatro archivos de registro:

- El bb2fa.log es el principal archivo de registro que incluye todos los mensajes que el servidor de BlackBerry 2FA escribe. Por ejemplo, incluye los mensajes de cierre e inicio, así como los mensajes relacionados con el progreso de la autenticación.
- key_log.txt es el archivo que contiene los mensajes relacionados con la creación y el estado de las claves que el servidor de BlackBerry 2FA requiere para proteger la información confidencial, como las contraseñas.
- bb2fa-audit.log es un archivo de auditoría delimitado por comas que registra cada solicitud de autenticación que el servidor de BlackBerry 2FA ha realizado.
- winrun_log.txt es el archivo que contiene los mensajes específicos del inicio y funcionamiento del servidor de BlackBerry 2FA cuando se ejecuta en los servicios de Windows.

BlackBerry 2FA utiliza la herramienta de registro Apache log4j para el registro. De forma predeterminada, el servidor de BlackBerry 2FA escribe los mensajes de registro en el nivel de información.

El servidor de BlackBerry 2FA crea nuevos archivos de registro y auditoría a diario. Cuando se crea el archivo de registro o auditoría, el archivo de registro o auditoría anterior adquiere la marca de tiempo bb2fa.*<fecha>*.log o b2fa-audit.log.*<fecha>*.

Puede cambiar el nivel de registro y dónde BlackBerry 2FA almacena el archivo de registro y auditoría mediante el archivo log4j.properties en *<directorio_instalación>*\bb2fa-config. Para obtener más información, visite http://logging.apache.org/log4j/2.x/ para leer la *Guía del usuario Apache log4j 2*.

Auditoría de solicitudes de autenticación

Servidor de BlackBerry 2FA

El servidor de BlackBerry 2FA registra todas las solicitudes de autenticación que realiza en un archivo de registro de auditoría cuando la solicitud caduca. El archivo de registro de auditoría incluye la siguiente información sobre todas las solicitudes:

- Fecha
- Hora
- ID de transacción
- Nombre de cliente
- Dirección IP de cliente
- Nombre de usuario
- Opción de autenticación
- Dispositivos con BlackBerry 10 asignados al usuario
- Dispositivos de terceros asignados al usuario
- Dispositivos OS con BlackBerry asignados al usuario
- Dispositivo que haya respondido a la solicitud de autenticación
- Tiempo (en segundos) que llevó completar la solicitud de autenticación
- Resultado de la solicitud

Por ejemplo:

```
2015-11-05,13:27:17.822,50dbe1cc,radtest,10.135.41.74,caperez,ENTERPRISE_PW,
[BESNameOne:BB10:2fff369:OK],[BES12-TEST:THIRDPARTY: 1fdf6d37-4f21-4516-b43f-
c90be83f646c:OK],[BESNameOne:BBOS:2fff367:OK],[BBOS:2fff367],6.742,AUTH_SUCCEEDED
```

El archivo de registro de auditoría es un archivo delimitado por comas que puede abrirse en cualquier software que admita CSV. Se denomina archivo bb2fa-audit.log y se almacena en *<directorio_instalación>*\logs.

BlackBerry UEM

Para obtener más información sobre el registro de BlackBerry UEM, consulte el contenido de administración de BlackBerry UEM.

Centralización del registro o auditoría mediante syslog

Puede configurar el servidor de BlackBerry 2FA de manera que escriba sus archivos de registro, sus archivos de auditoría o ambos en un servidor syslog centralizado en vez de en archivos locales.

Nota: Esta tarea muestra una forma de centralizar el registro. Para obtener más información sobre cómo configurar el registro, visite http://logging.apache.org/log4j/2.x/ para leer la *Guía del usuario Apache log4j 2*.

1. Busque la carpeta <*directorio_instalación*>\bb2fa-config.
2. Realice una copia de seguridad del archivo log4j.properties.
3. Abra el archivo log4j.properties en un editor de texto.
4. Para enviar mensajes de registro a un servidor syslog central, realice las acciones siguientes:
   a) Cambie el valor de `log4j.rootLogger` a uno de los siguientes:
      - Para escribir mensajes de registro solo para un servidor syslog, `ALL, syslog`
      - Para escribir mensajes de registro de forma local y para un servidor syslog, `ALL, logfile, syslog`
   b) Agregue las siguientes líneas:

      ```
      log4j.appender.syslog=org.apache.log4j.net.SyslogAppender
      log4j.appender.SYSLOG.Threshold=INFO
      log4j.appender.SYSLOG.syslogHost=<nombrehost>:<port>
      log4j.appender.SYSLOG.layout=org.apache.log4j.PatternLayout
      log4j.appender.SYSLOG.layout.ConversionPattern=[%-5p] %c - %m%n
      ```

   c) Establezca el valor de `log4j.appender.syslog.syslogHost` en el nombre del host y el puerto de su servidor syslog.
   d) Opcionalmente, para eliminar un registro local, elimine las líneas siguientes:

      ```
      # Salida del archivo de registro
      log4j.appender.logfile=org.apache.log4j.DailyRollingFileAppender
      log4j.appender.logfile.layout=org.apache.log4j.PatternLayout
      log4j.appender.logfile.layout.ConversionPattern=%d{ISO8601} [%-5p] (%t) %c -
       %m%n
      log4j.appender.logfile.datePattern='.'yyyy-MM-dd
      log4j.appender.logfile.Threshold = INFO
      log4j.appender.logfile.append=true
      log4j.appender.logfile.File=logs/bb2fa.log
      ```

5. Para enviar mensajes de auditoría a un servidor syslog central, realice las acciones siguientes:
   a) Cambie el valor de `log4j.logger.auditLogger` a uno de los siguientes:
      - Para escribir un mensaje de auditoría solo para un servidor syslog, `ALL, auditsyslog`

- Para escribir mensajes de auditoría de forma local y para un servidor syslog, `ALL, auditfile, auditsyslog`

b) Agregue las siguientes líneas:

```
log4j.appender.auditsyslog=org.apache.log4j.net.SyslogAppender
log4j.appender.auditsyslog.Threshold = INFO
log4j.appender.auditsyslog.syslogHost=<nombrehost>:<port>
log4j.appender.auditsyslog.layout=org.apache.log4j.PatternLayout
log4j.appender.auditsyslog.layout.ConversionPattern=%d{yyyy-MM-dd},
%d{HH:mm:ss.SSS},%m%n
```

c) Establezca el valor de `log4j.appender.syslog.syslogHost` en el nombre del host y el puerto de su servidor syslog. Para el archivo de auditoría, debe utilizar un puerto diferente al del archivo de registro.

d) Opcionalmente, para eliminar una auditoría local, elimine las líneas siguientes:

```
# Salida del archivo de auditoría
log4j.appender.auditfile=org.apache.log4j.DailyRollingFileAppender
log4j.appender.auditfile.layout=org.apache.log4j.PatternLayout
log4j.appender.auditfile.layout.ConversionPattern=%d{yyyy-MM-dd},
%d{HH:mm:ss.SSS},%m%n
log4j.appender.auditfile.datePattern='.'yyyy-MM-dd
log4j.appender.auditfile.Threshold = INFO
log4j.appender.auditfile.append=true
log4j.appender.auditfile.File=logs/bb2fa-audit.log
```

6. Guarde los cambios.
7. En los servicios de Windows, reinicie el servicio de BlackBerry 2FA.

Ejemplo del archivo log4j.properties con registro en syslog y local

```
log4j.rootLogger=ALL, logfile, syslog

log4j.logger.auditLogger=ALL, auditfile, auditsyslog

# Queremos controlar la salida Apache CFX y Jetty,
# que están muy detalladas en el nivel de depuración
log4j.logger.org.apache.cxf=INFO
log4j.logger.org.eclipse.jetty=INFO

# Redirija registros a un archivo de registro local
log4j.appender.logfile=org.apache.log4j.DailyRollingFileAppender
log4j.appender.logfile.layout=org.apache.log4j.PatternLayout
log4j.appender.logfile.layout.ConversionPattern=%d{ISO8601} [%-5p] (%t) %c - %m%n
log4j.appender.logfile.datePattern='.'yyyy-MM-dd
log4j.appender.logfile.Threshold = INFO
log4j.appender.logfile.append=true
log4j.appender.logfile.File=logs/bb2fa.log

# Redirija registros a un servidor syslog remoto
log4j.appender.syslog=org.apache.log4j.net.SyslogAppender
log4j.appender.syslog.Threshold = INFO
log4j.appender.syslog.syslogHost=syslog.example.com:514
log4j.appender.syslog.layout=org.apache.log4j.PatternLayout
log4j.appender.syslog.layout.ConversionPattern=[%-5p] %c - %m%n

# Redirija mensajes de auditoría a un archivo de auditoría local
log4j.appender.auditfile=org.apache.log4j.DailyRollingFileAppender
log4j.appender.auditfile.layout=org.apache.log4j.PatternLayout
```

```
log4j.appender.auditfile.layout.ConversionPattern=%d{yyyy-MM-dd},%d{HH:mm:ss.SSS},
%m%n
log4j.appender.auditfile.datePattern='.'yyyy-MM-dd
log4j.appender.auditfile.Threshold = INFO
log4j.appender.auditfile.append=true
log4j.appender.auditfile.File=logs/bb2fa-audit.log

# Redirija mensajes de auditoría a un servidor syslog remoto
#(puede que necesite un puerto diferente para generar un archivo diferente)
log4j.appender.auditsyslog=org.apache.log4j.net.SyslogAppender
log4j.appender.auditsyslog.Threshold = INFO
log4j.appender.auditsyslog.syslogHost=syslog.example.com:515
log4j.appender.auditsyslog.layout=org.apache.log4j.PatternLayout
log4j.appender.auditsyslog.layout.ConversionPattern=%d{yyyy-MM-dd},
%d{HH:mm:ss.SSS},%m%n
```

Opciones de autenticación

BlackBerry 2FA ofrece las siguientes opciones de autenticación:

Nota: Si se le asigna a un usuario alguna opción de dos factores, también tendrá permitido utilizar automáticamente identificadores OTP si se le asigna uno.

Opción de autenticación	Descripción	Resulta útil cuando
Autenticación de dos factores mediante contraseña de empresa	Cuando un usuario inicia sesión, proporciona un nombre de usuario y una contraseña de directorio y se le pide que confirme la solicitud de autenticación en el dispositivo. Si se le asigna a un usuario esta opción, tendrá permitido utilizar automáticamente identificadores OTP si se le asigna uno. Esta opción es compatible con todos los dispositivos.	Su empresa considera la seguridad como el objetivo más importante de cualquier implementación.
Autenticación de dos factores mediante contraseña de dispositivo pasiva	Cuando un usuario inicia sesión, solo proporciona un nombre de usuario y se le pide que confirme la solicitud de autenticación. Si el dispositivo está bloqueado, el usuario debe proporcionar la contraseña del dispositivo antes de poder confirmar la solicitud. Si se le asigna a un usuario esta opción, tendrá permitido utilizar automáticamente identificadores OTP si se le asigna uno. En el caso de dispositivos con BlackBerry 10, los usuarios deben proporcionar la contraseña del espacio de trabajo si este se encuentra bloqueado. Esta opción es compatible con todos los dispositivos.	Su empresa considera la utilidad como el objetivo más importante de cualquier implementación.

Opción de autenticación	Descripción	Resulta útil cuando
Autenticación de dos factores mediante contraseña de dispositivo activa	Cuando un usuario inicia sesión, solo proporciona un nombre de usuario y se le pide que confirme la solicitud de autenticación en el dispositivo. El usuario debe proporcionar siempre la contraseña del dispositivo antes de poder confirmar la solicitud. Si se le asigna a un usuario esta opción, tendrá permitido utilizar automáticamente identificadores OTP si se le asigna uno. En el caso de dispositivos con BlackBerry 10, los usuarios deben proporcionar la contraseña del espacio de trabajo. Esta opción solo es compatible con dispositivos con BlackBerry 10 y BlackBerry OS (versiones 6.0 a 7.1).	Su organización hace hincapié en la utilidad, pero quiere ofrecer protección frente a que alguien coja y desbloquee el dispositivo y acepte la solicitud del dispositivo.
Autenticación de factor único mediante contraseña de empresa	Los usuarios solo inician sesión mediante la autenticación de Microsoft Active Directory.	• El usuario no tiene ningún dispositivo. • El usuario ha olvidado o perdido su dispositivo. • El usuario no tiene que utilizar un segundo factor de autenticación.

Nota: En la versión 2.5 de BlackBerry 2FA puede configurar las opciones de autenticación de usuario de varias formas diferentes. De forma predeterminada, las opciones de autenticación se configuran mediante un perfil de BlackBerry 2FA en BlackBerry UEM. Sin embargo, puede anular esta configuración predeterminada para las solicitudes de autenticación enviadas a través de la API de REST o mediante puertas de enlace VPN y otros clientes RADIUS. Para obtener más información, consulte Configuración de la conectividad del extremo de la API de REST o Configuración de una conexión entre el servidor de BlackBerry 2FA y una puerta de enlace VPN.

Nombres de usuario, contraseñas y directorios

BlackBerry 2FA autentica a los usuarios disponibles en un directorio. El servidor de BlackBerry 2FA y BlackBerry UEM están conectados a esos directorios. En función de la configuración de estas conexiones, BlackBerry 2FA admite cuatro tipos de usuario:

- Usuarios en un dominio Microsoft Active Directory que esté conectado a un servidor de BlackBerry 2FA y BlackBerry UEM
- Usuarios en un dominio Microsoft Active Directory que no esté conectado a un servidor de BlackBerry 2FA, pero que esté conectado a BlackBerry UEM
- Usuarios en un directorio de LDAP que esté conectado a BlackBerry UEM
- Usuarios en un directorio de BlackBerry UEM local

Cuando un usuario inicia sesión, debe proporcionar un nombre de usuario y, opcionalmente, una contraseña.

Nombre de usuario

El nombre de usuario debe corresponder a una sola entrada de usuario en un directorio. Si no es así, la solicitud de autenticación no se realizará. Para especificar el directorio en el que reside el usuario, este debe ser identificado según los siguientes nombres de usuario para cada tipo de usuario:

- Los siguientes nombres de usuario se admiten para los usuarios en un dominio Microsoft Active Directory que está conectado a un servidor BlackBerry 2FA y BlackBerry UEM. Estos usuarios pueden autenticarse mediante el uso de PAP, MSCHAPv1, MSCHAPv2 y EAP-MSCHAPv2; además, pueden configurarse para utilizar grupos de autorización para cada cliente API de REST y grupos de anulación de autenticación para cada puerta de enlace VPN.

  <nombre de usuario> (p. ej., jsmith)

  <nombre de usuario>@<nombre de dominio NetBIOS> (p. ej., jsmith@company)

  <nombre de dominio NetBIOS>\<nombre de usuario> (p. ej., company\jsmith)

  <dirección de correo> (p. ej., jsmith@company.com)
- Los siguientes nombres de usuario se admiten para los usuarios de un dominio Microsoft Active Directory que no está conectado a un servidor BlackBerry 2FA, pero que está conectado a BlackBerry UEM. Estos usuarios pueden autenticarse usando solo PAP.

  <nombre de usuario> (p. ej., jsmith)

  <nombre de usuario>@<nombre de dominio NetBIOS> (p. ej., jsmith@company)

  <nombre de dominio NetBIOS>\<nombre de usuario> (p. ej., company\jsmith)

  <dirección de correo> (p. ej., jsmith@company.com)
- Los siguientes nombres de usuario se admiten para los usuarios en un directorio de LDAP que está conectado a BlackBerry UEM. Estos usuarios deben autenticarse con PAP.

  Nota: El servidor de BlackBerry 2FA no puede conectarse a este directorio.

  <nombre de usuario> (p. ej., jsmith)

  <nombre de usuario>@<FQDN del directorio> (p. ej., jsmith@company.ldap.net)

  <FQDN del directorio>\<nombre de usuario> (p. ej., company.ldap.net\jsmith)

  <dirección de correo> (p. ej., jsmith@company.com)
- Los siguientes nombres de usuario son admitidos para los usuarios en un directorio de BlackBerry UEM local. Estos usuarios deben autenticarse con PAP.

  Nota: El servidor de BlackBerry 2FA no puede conectarse a este directorio.

  <nombre de usuario> (p. ej., jsmith)

  <nombre de usuario>@local (p. ej., jsmith@local)

local\<nombre de usuario> (p. ej., local\jsmith)

<dirección de correo> (p. ej., jsmith@company.com)

Contraseña

Cuando un usuario inicia sesión, debe proporcionar una contraseña de directorio en función de la opción de autenticación que utilice por configuración.

Si un usuario se está autenticando con un identificador de contraseña de un solo uso (OTP), deben proporcionar la OTP y la contraseña del directorio independientemente de la opción de autenticación en dos fases que utilice por configuración.

- Para iniciar sesión en una VPN, el usuario debe introducir la OTP y la contraseña del directorio en el campo contraseña. Primero se escribe la OTP y después la contraseña del directorio sin espacios ni separadores.
- Cuando inicie sesión desde un cliente conectado a una API de REST, el usuario debe introducir la contraseña del directorio en el campo contraseña y, a continuación, introducir la OTP en un campo dedicado a ello.

Puertas de enlace VPN

Puede usar la página de configuración del servidor de BlackBerry 2FA en la consola de gestión de BlackBerry UEM para crear una puerta de enlace VPN. La conexión entre una puerta de enlace VPN y el servidor de BlackBerry 2FA se establece mediante el uso de RADIUS. Para obtener más información, consulte Configuración de una conexión entre el servidor de BlackBerry 2FA y una puerta de enlace VPN.

Extremo API de REST

El servidor de BlackBerry 2FA tiene un extremo de la API de REST que extiende BlackBerry 2FA a servicios personalizados como aplicaciones web y aplicaciones cliente SIP. Puede utilizar la página de configuración del servidor de BlackBerry 2FA en la consola de gestión de BlackBerry UEM para crear un cliente de REST. Para obtener más información, consulte Configuración de la conectividad del extremo de la API de REST.

Glosario

API	Application Programming Interface (Interfaz de programación de aplicaciones)
CA	autoridad de certificación
DNS	Domain Name System (Sistema de nombres de dominio)
ECDH	Elliptic Curve Diffie-Hellman (Curva elíptica Diffie-Hellman)
EAP	Extensible Authentication Protocol (Protocolo de autenticación extensible)
EMM	Gestión de movilidad empresarial
FQDN	Fully Qualified Domain Name (Nombre de dominio completo)
HTTP	Hypertext Transfer Protocol (Protocolo de transferencia de hipertexto)
HTTPS	Hypertext Transfer Protocol over Secure Sockets Layer (Protocolo de transferencia de hipertexto a través de un nivel de socket seguro)
IP	Internet Protocol (Protocolo de Internet)
política de TI	Una política de TI consiste en varias reglas que controlan las características de seguridad y el comportamiento de los dispositivos.
IKE	Intercambio de claves de Internet (Internet Key Exchange)
MAM	administración de aplicaciones móviles
MDM	Mobile Device Management (Administración de dispositivos móviles)
MS-CHAP	Microsoft Challenge Handshake Authentication Protocol (Protocolo de autenticación por desafío mutuo de Microsoft)
NAS	almacenamiento conectado a la red
NTLM	Personal Information Management (Gestor de LAN NT)

OTP	contraseña de un solo uso
PAP	Push Access Protocol (Protocolo de acceso push)
RADIUS	Remote Authentication Dial In User Service (service utilisateur de connexion par authentification à distance)
REST	Transferencia de estado representacional
SAML	Security Assertion Markup Language
SIP	Session Initiation Protocol (Protocolo de inicio de sesión)
SSL	Secure Sockets Layer (Capa de sockets seguros)
TLS	Transport Layer Security (Seguridad de capa de transporte)
UEM	Gestión unificada de extremos
VPN	virtual private network (red privada virtual)

Aviso legal

OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN INCLUDING WITHOUT LIMITATION ANY OF THE FOLLOWING DAMAGES: DIRECT, CONSEQUENTIAL, EXEMPLARY, INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, OR AGGRAVATED DAMAGES, DAMAGES FOR LOSS OF PROFITS OR REVENUES, FAILURE TO REALIZE ANY EXPECTED SAVINGS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, LOSS OF BUSINESS OPPORTUNITY, OR CORRUPTION OR LOSS OF DATA, FAILURES TO TRANSMIT OR RECEIVE ANY DATA, PROBLEMS ASSOCIATED WITH ANY APPLICATIONS USED IN CONJUNCTION WITH BLACKBERRY PRODUCTS OR SERVICES, DOWNTIME COSTS, LOSS OF THE USE OF BLACKBERRY PRODUCTS OR SERVICES OR ANY PORTION THEREOF OR OF ANY AIRTIME SERVICES, COST OF SUBSTITUTE GOODS, COSTS OF COVER, FACILITIES OR SERVICES, COST OF CAPITAL, OR OTHER SIMILAR PECUNIARY LOSSES, WHETHER OR NOT SUCH DAMAGES WERE FORESEEN OR UNFORESEEN, AND EVEN IF BLACKBERRY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, BLACKBERRY SHALL HAVE NO OTHER OBLIGATION, DUTY, OR LIABILITY WHATSOEVER IN CONTRACT, TORT, OR OTHERWISE TO YOU INCLUDING ANY LIABILITY FOR NEGLIGENCE OR STRICT LIABILITY.

THE LIMITATIONS, EXCLUSIONS, AND DISCLAIMERS HEREIN SHALL APPLY: (A) IRRESPECTIVE OF THE NATURE OF THE CAUSE OF ACTION, DEMAND, OR ACTION BY YOU INCLUDING BUT NOT LIMITED TO BREACH OF CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY OR ANY OTHER LEGAL THEORY AND SHALL SURVIVE A FUNDAMENTAL BREACH OR BREACHES OR THE FAILURE OF THE ESSENTIAL PURPOSE OF THIS AGREEMENT OR OF ANY REMEDY CONTAINED HEREIN; AND (B) TO BLACKBERRY AND ITS AFFILIATED COMPANIES, THEIR SUCCESSORS, ASSIGNS, AGENTS, SUPPLIERS (INCLUDING AIRTIME SERVICE PROVIDERS), AUTHORIZED BLACKBERRY DISTRIBUTORS (ALSO INCLUDING AIRTIME SERVICE PROVIDERS) AND THEIR RESPECTIVE DIRECTORS, EMPLOYEES, AND INDEPENDENT CONTRACTORS.

IN ADDITION TO THE LIMITATIONS AND EXCLUSIONS SET OUT ABOVE, IN NO EVENT SHALL ANY DIRECTOR, EMPLOYEE, AGENT, DISTRIBUTOR, SUPPLIER, INDEPENDENT CONTRACTOR OF BLACKBERRY OR ANY AFFILIATES OF BLACKBERRY HAVE ANY LIABILITY ARISING FROM OR RELATED TO THE DOCUMENTATION.

Prior to subscribing for, installing, or using any Third Party Products and Services, it is your responsibility to ensure that your airtime service provider has agreed to support all of their features. Some airtime service providers might not offer Internet browsing functionality with a subscription to the BlackBerry® Internet Service. Check with your service provider for availability, roaming arrangements, service plans and features. Installation or use of Third Party Products and Services with BlackBerry's products and services may require one or more patent, trademark, copyright, or other licenses in order to avoid infringement or violation of third party rights. You are solely responsible for determining whether to use Third Party Products and Services and if any third party licenses are required to do so. If required you are responsible for acquiring them. You should not install or use Third Party Products and Services until all necessary licenses have been acquired. Any Third Party Products and Services that are provided with BlackBerry's products and services are provided as a convenience to you and are provided "AS IS" with no express or implied conditions, endorsements, guarantees, representations, or warranties of any kind by BlackBerry and BlackBerry assumes no liability whatsoever, in relation thereto. Your use of Third Party Products and Services shall be governed by and subject to you agreeing to the terms of separate licenses and other agreements applicable thereto with third parties, except to the extent expressly covered by a license or other agreement with BlackBerry.

The terms of use of any BlackBerry product or service are set out in a separate license or other agreement with BlackBerry applicable thereto. NOTHING IN THIS DOCUMENTATION IS INTENDED TO SUPERSEDE ANY EXPRESS WRITTEN AGREEMENTS OR WARRANTIES PROVIDED BY BLACKBERRY FOR PORTIONS OF ANY BLACKBERRY PRODUCT OR SERVICE OTHER THAN THIS DOCUMENTATION.

BlackBerry Enterprise Software incorporates certain third-party software. The license and copyright information associated with this software is available at http://worldwide.blackberry.com/legal/thirdpartysoftware.jsp.

BlackBerry Limited
2200 University Avenue East

Waterloo, Ontario
Canada N2K 0A7

BlackBerry UK Limited
200 Bath Road
Slough, Berkshire SL1 3XE
United Kingdom

Published in Canada