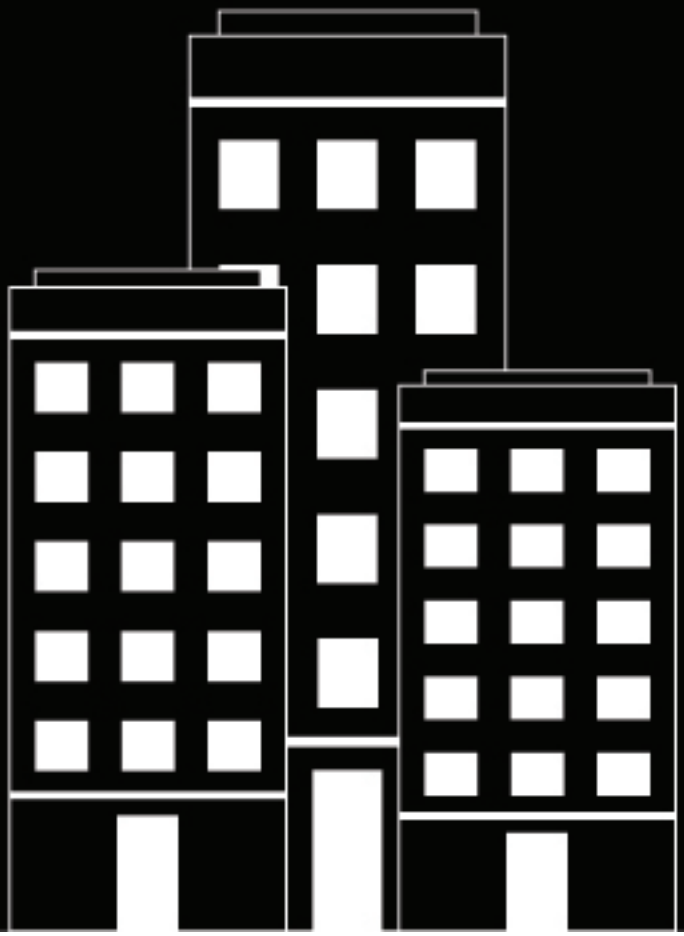

BlackBerry UEM

Protección de las conexiones de red

Administración

12.17

Contents

Gestión de Wi-Fi, VPN, BlackBerry Secure Connect Plus y otras conexiones de trabajo

Puede utilizar los perfiles para configurar y administrar las conexiones de trabajo para los dispositivos de la empresa. Las conexiones de trabajo definen el modo en que los dispositivos se conectan a los recursos de trabajo en el entorno de la empresa, tales como servidores de correo, servidores proxy, redes Wi-Fi y VPN. Puede especificar la configuración de los dispositivos con iOS, macOS, Android y Windows 10 en el mismo perfil y, a continuación, asignar el perfil a las cuentas de usuarios, a los grupos de usuarios o a los grupos de dispositivos.

Administración de las conexiones de trabajo mediante los perfiles

Puede configurar cómo los dispositivos se conectan a los recursos de trabajo mediante los siguientes perfiles:

Perfil	Descripción
Wi-Fi	En un perfil de Wi-Fi se especifica la forma de conexión de los dispositivos a una red Wi-Fi de trabajo.
VPN	En un perfil de VPN se especifica la forma de conexión de los dispositivos a una red VPN de trabajo.
Proxy	En un perfil de proxy se puede especificar la forma de uso de un servidor proxy de los dispositivos para acceder a servicios web en internet o en una red de trabajo.
Conectividad de la empresa	El perfil de conectividad de la empresa especifica el método de conexión de los dispositivos con los recursos de su empresa mediante la conectividad de la empresa y BlackBerry Secure Connect Plus.
BlackBerry 2FA	Un perfil de BlackBerry 2FA permite la autenticación de dos factores para los usuarios y especifica la configuración de las funciones de autenticación previa y de autorrescate.
Extensión de registro único	En un perfil de extensión de registro único se especifica cómo autenticar dispositivos con iOS y iPadOS con dominios seguros automáticamente después de que los usuarios escriban el nombre de usuario y la contraseña por primera vez.
Perfil de conectividad de BlackBerry Dynamics	Un perfil de conectividad de BlackBerry Dynamics define las conexiones de red, los dominios de Internet, los rangos de dirección IP y los servidores de aplicaciones a los que los dispositivos se pueden conectar cuando se usan aplicaciones de BlackBerry Dynamics.
Correo	En un perfil de correo electrónico se especifica cómo se conectan los dispositivos al servidor de correo de trabajo y cómo sincronizan los mensajes de correo, las entradas del calendario y los datos del organizador mediante Exchange ActiveSync o IBM Notes Traveler.
IMAP/correo electrónico POP3	Un perfil de correo IMAP/POP3 para especificar cómo los dispositivos se conectan al servidor de correo IMAP o POP3 y cómo sincronizan los mensajes de correo.

Procedimiento recomendado: creación de perfiles de conexión de trabajo

Algunos perfiles de conexión de trabajo pueden incluir uno o más perfiles asociados. Al especificar un perfil asociado, se vincula un perfil a un perfil de conexión de trabajo y los dispositivos deberán utilizar el perfil asociado al utilizar el perfil de conexión de trabajo.

Considere las siguientes directrices:

- Determine qué conexiones de trabajo se requieren para los dispositivos en la empresa.
- Cree perfiles que se puedan asociar a otros perfiles antes de crear los perfiles de conexión de trabajo que los utilizan.
- Utilice variables cuando proceda.

Puede asociar perfiles de certificado y de proxy a varios perfiles de conexión de trabajo. Debe crear perfiles en el siguiente orden:

1. Perfiles de certificado
2. Perfiles de proxy
3. Perfiles de conexión de trabajo tales como correo, VPN y Wi-Fi

Por ejemplo, si crea un perfil de Wi-Fi en primer lugar, no se puede asociar un perfil de proxy al perfil de Wi-Fi cuando éste se crea. Después de crear un perfil de proxy, debe cambiar el perfil de Wi-Fi para asociarlo al perfil de proxy.

Configuración de las redes Wi-Fi de trabajo para dispositivos

Puede utilizar un perfil de Wi-Fi para especificar el modo en que los dispositivos se conectan a una red Wi-Fi de trabajo detrás del firewall. Se puede asignar un perfil de Wi-Fi a cuentas de usuarios, a grupos de usuarios y a grupos de dispositivos.

De forma predeterminada, tanto las aplicaciones de trabajo como las personales pueden utilizar los perfiles Wi-Fi guardados en el dispositivo para conectarse a la red de la empresa.

Creación de un perfil de Wi-Fi

La configuración del perfil obligatorio varía para cada tipo de dispositivo y depende del tipo de seguridad Wi-Fi y del protocolo de autenticación que seleccione.

Antes de empezar:

- Si los dispositivos utilizan la autenticación basada en certificados para conexiones Wi-Fi de trabajo, cree un perfil de certificado de CA y asígnelo a las cuentas de usuario, a los grupos de usuarios o a los grupos de dispositivos. Para enviar certificados de cliente a dispositivos, cree un SCEP, un certificado compartido o un perfil de credenciales de usuario para asociarlo al perfil Wi-Fi.
  Nota: Los dispositivos Samsung Knox Workspace no son compatibles con el uso de los certificados que BlackBerry UEM ha enviado a los dispositivos para la autenticación Wi-Fi. Los usuarios deben configurar manualmente la autenticación basada en certificados en los dispositivos Samsung Knox Workspace.
- Para los dispositivos con iOS, iPadOS, macOS y Android Enterprise que utilizan un servidor proxy para las conexiones Wi-Fi de trabajo, cree un perfil de proxy para asociarlo al perfil de Wi-Fi.

1. En la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Redes y conexiones > Wi-Fi**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil de Wi-Fi. Dicha información se muestra en los dispositivos.
5. En el campo **SSID**, escriba el nombre de red de una red Wi-Fi.
6. Si la red Wi-Fi no difunde el SSID, seleccione la casilla de verificación **Red oculta**.
7. Realice las acciones siguientes:
   a) Haga clic en la pestaña de un tipo de dispositivo.
   b) Configure los valores adecuados para cada configuración del perfil para que coincidan con la configuración Wi-Fi del entorno de la empresa. Si la empresa requiere que los usuarios proporcionen un nombre de usuario y una contraseña para conectarse a la red Wi-Fi y el perfil es para varios usuarios, en el campo **Nombre de usuario** escriba `%UserName%`.
8. Repita el paso 7 para cada tipo de dispositivo en la empresa.
9. Haga clic en **Agregar**.

Ajustes del perfil de Wi-Fi

Puede utilizar una variable en cualquier ajuste de perfil que sea un campo de texto para hacer referencia a un valor en lugar de especificar el valor real. Los perfiles de Wi-Fi son compatibles con los siguientes tipos de dispositivos:

- iOS
- iPadOS
- macOS
- Android
- Windows

Común: ajustes del perfil Wi-Fi

Común: ajuste del perfil Wi-Fi	Descripción
SSID	Esta configuración especifica el nombre de una red Wi-Fi y sus puntos de acceso inalámbrico. El SSID distingue mayúsculas de minúsculas y debe contener caracteres alfanuméricos. Los valores posibles están limitados a 32 caracteres.
Red oculta	En la configuración se especifica si la red Wi-Fi oculta el SSID.

iOS y macOS: Ajustes del perfil de Wi-Fi

La configuración para iOS también se aplica a los dispositivos con iPadOS.

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

iOS y macOS: Configuración de perfil de Wi-Fi	Descripción
Aplicar perfil a	Esta configuración especifica si el perfil Wi-Fi de un dispositivo macOS se aplica a la cuenta de usuario o al dispositivo. Valores posibles: • Usuario • Dispositivo Esta configuración solo es válida para macOS.
Conexión automática a la red	Esta configuración especifica si un dispositivo puede conectarse automáticamente a la red Wi-Fi.
Desactivar la selección aleatoria de dirección MAC	Esta configuración especifica si los dispositivos pueden seleccionar aleatoriamente sus direcciones MAC al unirse a la red Wi-Fi. Esta configuración se aplica únicamente a los dispositivos que ejecutan iOS y iPadOS 14 y posteriores.
Perfil proxy asociado	Esta configuración especifica el perfil de proxy asociado que un dispositivo debe utilizar para conectarse al servidor proxy cuando el dispositivo está conectado a la red Wi-Fi.

iOS y macOS: Configuración de perfil de Wi-Fi	Descripción
Tipo de red	Esta configuración especifica la configuración para la red Wi-Fi. Las configuraciones del punto de acceso se aplican únicamente a dispositivos con iOS, iPadOS y macOS. Si selecciona una de las opciones de punto de acceso, no utilice el mismo perfil Wi-Fi para configurar los ajustes de otros tipos de dispositivos. Valores posibles: • Estándar • Punto de acceso heredado • Punto de acceso 2.0 El valor predeterminado es "Estándar".
Nombre de operador mostrado	Esta configuración especifica el nombre descriptivo del operador del punto de acceso. Esta configuración es válida únicamente si la opción "Tipo de red" se establece en "Punto de acceso 2.0".
Nombre de dominio	Esta configuración especifica el nombre del dominio del operador del punto de acceso. Esta configuración es válida únicamente si la opción "Tipo de red" se establece en "Punto de acceso 2.0". No se requiere el ajuste "SSID" cuando utiliza este ajuste.
Identificadores de empresa de los consorcios de roaming	Esta configuración especifica los identificadores de empresa de los consorcios de roaming y proveedores de servicios que son accesibles a través del punto de acceso. Esta configuración es válida únicamente si la opción "Tipo de red" se establece en "Punto de acceso 2.0".
Nombres de dominio NAI	En la configuración se especifican los nombres de dominio NAI que pueden autenticar un dispositivo. Esta configuración es válida únicamente si la opción "Tipo de red" se establece en "Punto de acceso 2.0".
MCC/MNC	Esta configuración especifica las combinaciones MCC/MNC que identifican a los operadores de red móvil. Cada valor debe contener exactamente seis dígitos. Esta configuración es válida únicamente si la opción "Tipo de red" se establece en "Punto de acceso 2.0".
Permitir la conexión a redes de socios de roaming	Esta configuración especifica si un dispositivo puede conectarse a los socios de roaming para obtener un punto de acceso. Esta configuración es válida únicamente si la opción "Tipo de red" se establece en "Punto de acceso 2.0".

iOS y macOS: Configuración de perfil de Wi-Fi	Descripción
Tipo de seguridad	Esta configuración especifica el tipo de seguridad que utiliza la red Wi-Fi. Si el ajuste "Tipo de red" se establece en "Punto de acceso 2.0", este ajuste se establece en "WPA2-Enterprise". Valores posibles: • Ninguno • WEP personal • Empresa con WEP • WPA-Personal • WPA-Enterprise • WPA2-Personal • WPA2-Enterprise • WPA3-Personal • WPA3-Enterprise El valor predeterminado es "Ninguno".
Clave WEP	Esta configuración especifica la clave WEP para la red Wi-Fi. La clave WEP debe contener 10 o 26 caracteres hexadecimales (0-9, A-F) o bien 5 o 13 caracteres alfanuméricos (0-9, A-Z). Ejemplos de valores de clave hexadecimal son ABCDEF0123 o ABCDEF0123456789ABCDEF0123. Ejemplos de valores de clave alfanumérica son abCD5 o abCDefGHijKL1. Esta configuración es válida únicamente si la opción "Tipo de seguridad" se establece en "WEP personal".
Clave compartida previamente	Esta configuración especifica la clave compartida previamente para la red Wi-Fi. Esta configuración es válida únicamente si la opción "Tipo de seguridad" se establece en "WPA-Personal," "WPA2-Personal" o "WPA3-Personal".
Protocolos	

iOS y macOS: Configuración de perfil de Wi-Fi	Descripción
Protocolo de autenticación	Esta configuración especifica los métodos EAP que debe admitir la red Wi-Fi. Puede seleccionar múltiples métodos EAP. Esta configuración es válida únicamente si la opción "Tipo de seguridad" se establece en "Empresa con WEP", "WPA-Enterprise", "WPA2-Enterprise" o "WPA3-Enterprise". Selecciones posibles: • TLS • TTLS • LEAP • PEAP • EAP-FAST • EAP-SIM • EAP-AKA
Autenticación interna	Esta configuración especifica el método de autenticación interna que desea utilizar con TTLS. Esta configuración es válida únicamente si la opción "Protocolo de autenticación" se establece en "TTLS". Valores posibles: • Ninguno • PAP • CHAP • MS-CHAP • MS-CHAPv2 • EAP El valor predeterminado es "MS-CHAPv2".
Utilizar PAC	Esta configuración especifica si el método EAP-FAST debe utilizar credenciales de acceso protegido. Esta configuración es válida únicamente si la opción "Protocolo de autenticación" se establece en "EAP-FAST".
Proporcionar PAC	Esta configuración especifica si el método EAP-FAST debe permitir el suministro de PAC. Esta configuración es válida únicamente si el "Protocolo de autenticación" se establece en "EAP-FAST" y se selecciona la opción "Utilizar PAC".
Proporcionar PAC de forma anónima	Esta configuración especifica si el método EAP-FAST debe permitir el suministro anónimo de PAC. Esta configuración es válida únicamente si la opción "Protocolo de autenticación" se establece en "EAP-FAST" y se selecciona la opción "Utilizar PAC" y la opción "Proporcionar PAC".

iOS y macOS: Configuración de perfil de Wi-Fi	Descripción
Autenticación	
Identidad externa para TTLS, PEAP y EAP-FAST	Esta configuración especifica la identidad externa para un usuario enviado en texto no cifrado. Puede especificar un nombre de usuario anónimo para ocultar la identidad real del usuario (por ejemplo, anónimo). El túnel cifrado se utiliza para autenticar el nombre de usuario real con la red Wi-Fi. Si la identidad externa incluye el nombre de dominio kerberos para distribuir la solicitud, debe ser el dominio kerberos real del usuario (por ejemplo, anónimo@ejemplo.com). Esta configuración es válida únicamente si la opción "Protocolo de autenticación" se establece en "TTLS", "PEAP" o "EAP-FAST".
Utilizar contraseña incluida en el perfil de Wi-Fi	Esta configuración especifica si desea que el perfil de Wi-Fi incluya la contraseña para la autenticación. Esta configuración es válida únicamente si la opción "Tipo de seguridad" se establece en "Empresa con WEP", "WPA-Enterprise", "WPA2-Enterprise" o "WPA3-Enterprise".
Contraseña	En la configuración se especifica la contraseña que un dispositivo debe utilizar para autenticar con la red Wi-Fi. Esta configuración es válida únicamente si se ha seleccionado la opción "Utilizar contraseña incluida en el perfil de Wi-Fi".
Nombre de usuario	En la configuración se especifica el nombre de usuario que un dispositivo debe utilizar para autenticar con la red Wi-Fi. Si el perfil es para varios usuarios, puede especificar la variable %UserName%. Esta configuración es válida únicamente si la opción "Tipo de seguridad" se establece en "Empresa con WEP", "WPA-Enterprise", "WPA2-Enterprise" o "WPA3-Enterprise".
Tipo de autenticación	Esta configuración especifica el tipo de autenticación que un dispositivo debe utilizar para conectarse a la red Wi-Fi. Esta configuración es válida únicamente si la opción "Tipo de seguridad" se establece en "Empresa con WEP", "WPA-Enterprise", "WPA2-Enterprise" o "WPA3-Enterprise". Valores posibles: • Ninguno • Certificado compartido • SCEP • Credencial de usuario El valor predeterminado es "Ninguno".

iOS y macOS: Configuración de perfil de Wi-Fi	Descripción
Tipo de vinculación de certificado	Esta configuración especifica el tipo de vínculo para el certificado de cliente asociado al perfil de Wi-Fi. Esta configuración es válida únicamente si la opción "Tipo de autenticación" se establece en "Certificado compartido". Valores posibles: • Referencia única • Inyección variable El valor predeterminado es "Referencia única".
Perfil de certificado compartido	Esta configuración especifica el perfil de certificado compartido con el certificado de cliente que debe utilizar un dispositivo para realizar la autenticación con la red Wi-Fi. Esta configuración es válida únicamente si la opción "Tipo de vinculación de certificado" se establece en "Referencia única".
Nombre del certificado de cliente	Esta configuración especifica el nombre del certificado de cliente que debe utilizar un dispositivo para realizar la autenticación con la red Wi-Fi. Esta configuración es válida únicamente si la opción "Tipo de vinculación de certificado" se establece en "Inyección variable".
Perfil SCEP asociado	Esta configuración especifica el perfil SCEP asociado que un dispositivo debe utilizar para obtener un certificado de cliente con el objetivo de autenticarlo con la red Wi-Fi. Esta configuración es válida únicamente si la opción "Tipo de autenticación" se establece en "SCEP".
Perfil de credenciales de usuario asociado	Esta configuración especifica el perfil de credenciales de usuario asociado que debe utilizar un dispositivo para obtener un certificado de cliente con el objetivo de realizar la autenticación con la red Wi-Fi. Esta configuración es válida únicamente si la opción "Tipo de autenticación" se establece en "Credenciales del usuario".
Confiar	
Nombres comunes de certificado esperados por el servidor de autenticación	Esta configuración especifica los nombres comunes en el certificado que el servidor de autenticación debe enviar al dispositivo (por ejemplo, *.example.com). Esta configuración es válida únicamente si la opción "Tipo de seguridad" se establece en "Empresa con WEP", "WPA-Enterprise", "WPA2-Enterprise" o "WPA3-Enterprise".

iOS y macOS: Configuración de perfil de Wi-Fi	Descripción
Tipo de vinculación de certificado	Esta configuración especifica el tipo de vinculación para los certificados de confianza asociados al perfil de Wi-Fi. Esta configuración es válida únicamente si la opción "Tipo de seguridad" se establece en "Empresa con WEP", "WPA-Enterprise", "WPA2-Enterprise" o "WPA3-Enterprise". Valores posibles: • Referencia única • Inyección variable El valor predeterminado es "Referencia única".
Perfiles de certificado de CA	Esta configuración especifica los perfiles de certificado de CA con los certificados de confianza que debe utilizar un dispositivo para establecer una conexión de confianza con una red Wi-Fi. Esta configuración es válida únicamente si la opción "Tipo de vinculación de certificado" se establece en "Referencia única".
Nombres de certificados de confianza	Esta configuración especifica el nombre de los certificados de confianza que un dispositivo debe utilizar para establecer una conexión de confianza con una red Wi-Fi. Esta configuración es válida únicamente si la opción "Tipo de vinculación de certificado" se establece en "Inyección variable".
Confiar en las decisiones de los usuarios	Esta configuración especifica si un dispositivo debe solicitar al usuario que confíe en un servidor cuando no puede establecerse la cadena de confianza. Si no se selecciona este ajuste, solo se permitirán las conexiones a los servidores de confianza que especifique. Esta configuración es válida únicamente si la opción "Tipo de seguridad" se establece en "Empresa con WEP", "WPA-Enterprise", "WPA2-Enterprise" o "WPA3-Enterprise".
Desviar red cautiva	Esta configuración especifica si los dispositivos pueden desviar redes cautivas.
Activar marcado de QoS	Esta configuración especifica si puede activar el marcado L2 y L3 para el tráfico enviado a través de la red Wi-Fi.
Usar QoS para llamadas de FaceTime	Esta configuración especifica si el tráfico de audio y vídeo para llamadas de FaceTime puede utilizar el marcado L2 y L3.
Usar solo marcado L2 para tráfico de QoS	Esta configuración especifica si el tráfico enviado a través de la red Wi-Fi solo utiliza el marcado L2.
Aplicar marcado de QoS a aplicaciones seleccionadas	Esta configuración especifica los ID de paquete para aplicaciones que pueden utilizar el marcado L2 y L3.

Android: configuración del perfil de Wi-Fi

Android: configuración del perfil de Wi-Fi	Descripción
Perfil proxy asociado	En esta configuración se especifica el perfil de proxy asociado que utiliza un dispositivo con Android para conectarse al servidor proxy cuando el dispositivo está conectado a la red Wi-Fi. Los dispositivos Android 8.0 y versiones posteriores con Controles de MDM o Privacidad del usuario no son compatibles con perfiles de Wi-Fi con configuración de proxy. Si un dispositivo con uno de estos tipos de activación se actualiza a Android 8.0, los perfiles de Wi-Fi que tienen un perfil de proxy asociado se eliminarán del dispositivo.
BSSID	En esta configuración se especifica la dirección MAC de un punto de acceso inalámbrico de la red Wi-Fi.
DNS primario	En la configuración se especifica el servidor DNS primario con notación decimal con puntos (por ejemplo, 192.0.2.0). La configuración se aplica únicamente a los dispositivos que utilizan Samsung Knox cuando la dirección IP se asigna de forma estática por la red de la empresa.
DNS secundario	En la configuración se especifica el servidor DNS secundario con notación decimal con puntos (por ejemplo, 192.0.2.0). La configuración se aplica únicamente a los dispositivos que utilizan Samsung Knox cuando la dirección IP se asigna de forma estática por la red de la empresa.
Tipo de seguridad	En la configuración se especifica el tipo de seguridad que utiliza la red Wi-Fi. Valores posibles: • Ninguno • Personal • Empresa El valor predeterminado es "Ninguno".
Tipo de seguridad personal	En esta configuración se especifica el tipo de seguridad personal que utiliza la red Wi-Fi. Esta configuración es válida únicamente si la opción "Tipo de seguridad" se establece en "Personal". Valores posibles: • Ninguno • WEP personal • WPA-Personal/WPA2-Personal El valor predeterminado es "Ninguno".

Android: configuración del perfil de Wi-Fi	Descripción
Clave WEP	Esta configuración especifica la clave WEP para la red Wi-Fi. La clave WEP debe contener 10 o 26 caracteres hexadecimales (0-9, A-F) o bien 5 o 13 caracteres alfanuméricos (0-9, A-Z). Ejemplos de valores de clave hexadecimal son ABCDEF0123 o ABCDEF0123456789ABCDEF0123. Ejemplos de valores de clave alfanumérica son abCD5 o abCDefGHijKL1. Esta configuración es válida únicamente si la opción "Tipo de seguridad personal" se establece en "WEP personal".
Clave compartida previamente	Esta configuración especifica la clave compartida previamente para la red Wi-Fi. Esta configuración es válida únicamente si la opción "Tipo de seguridad personal" se establece en "WPA-Personal/WPA2-Personal".
Protocolo de autenticación	En esta configuración se especifica el método EAP que utiliza la red Wi-Fi. Esta configuración es válida únicamente si la opción "Tipo de seguridad" se establece en "Empresa". Valores posibles: • TLS • TTLS • PEAP • LEAP El valor predeterminado es "TLS". LEAP no es compatible con los dispositivos que utilizan Samsung Knox.
Autenticación interna	En la configuración se especifica el método de autenticación interna que desea utilizar con TTLS. Esta configuración es válida únicamente si la opción "Protocolo de autenticación" se establece en "TTLS". Valores posibles: • Ninguno • PAP • CHAP • MS-CHAP • MS-CHAPv2 • GTC El valor predeterminado es "MS-CHAPv2". CHAP no es compatible con los dispositivos que utilizan Samsung Knox.

Android: configuración del perfil de Wi-Fi	Descripción
Identidad externa de TTLS	En la configuración se especifica la identidad externa para un usuario enviado en texto no cifrado. Puede especificar un nombre de usuario anónimo para ocultar la identidad real del usuario (por ejemplo, anónimo). El túnel cifrado se utiliza para autenticar el nombre de usuario real con la red Wi-Fi. Si la identidad externa incluye el nombre de dominio kerberos para distribuir la solicitud, debe ser el dominio kerberos real del usuario (por ejemplo, anónimo@ejemplo.com). Esta configuración es válida únicamente si la opción "Protocolo de autenticación" se establece en "TTLS".
Identidad externa de PEAP	En la configuración se especifica la identidad externa para un usuario enviado en texto no cifrado. Puede especificar un nombre de usuario anónimo para ocultar la identidad real del usuario (por ejemplo, anónimo). El túnel cifrado se utiliza para autenticar el nombre de usuario real con la red Wi-Fi. Si la identidad externa incluye el nombre de dominio kerberos para distribuir la solicitud, debe ser el dominio kerberos real del usuario (por ejemplo, anónimo@ejemplo.com). Esta configuración es válida únicamente si la opción "Protocolo de autenticación" se establece en "PEAP".
Nombre de usuario	En la configuración se especifica el nombre de usuario que un dispositivo Android debe utilizar para autenticar con la red Wi-Fi. Si el perfil es para varios usuarios, puede especificar la variable %UserName%. Esta configuración es válida únicamente si la opción "Tipo de seguridad" se establece en "Empresa".
Utilizar contraseña incluida en el perfil de Wi-Fi	En la configuración se especifica si desea que el perfil de Wi-Fi incluya la contraseña para la autenticación. Esta configuración es válida únicamente si la opción "Tipo de seguridad" se establece en "Empresa".
Contraseña	En la configuración se especifica la contraseña que un dispositivo Android debe utilizar para autenticar con la red Wi-Fi. Esta configuración es válida únicamente si se ha seleccionado la opción "Utilizar contraseña incluida en el perfil de Wi-Fi".
Tipo de autenticación	En esta configuración se especifica el tipo de autenticación que utiliza un dispositivo con Android para conectarse a la red Wi-Fi. Esta configuración es válida únicamente si la opción "Tipo de seguridad" se establece en "Empresa". Valores posibles: • Ninguno • Certificado compartido • SCEP • Credencial de usuario El valor predeterminado es "Ninguno".

Android: configuración del perfil de Wi-Fi	Descripción
Tipo de vinculación de certificado	En la configuración se especifica el tipo de vínculo para el certificado de cliente asociado al perfil de Wi-Fi. Esta configuración es válida únicamente si la opción "Tipo de autenticación" se establece en "Certificado compartido". Valores posibles: • Referencia única • Inyección variable El valor predeterminado es "Referencia única".
Perfil de certificado compartido	En esta configuración se especifica el perfil de certificado compartido con el certificado de cliente que utiliza un dispositivo con Android para autenticarse con la red Wi-Fi. Esta configuración es válida únicamente si la opción "Tipo de vinculación de certificado" se establece en "Referencia única". El nombre del perfil de certificado compartido debe tener menos de 36 caracteres para los dispositivos que utilizan Knox Workspace.
Perfil SCEP asociado	En esta configuración se especifica el perfil SCEP asociado que utiliza un dispositivo con Android para obtener un certificado de cliente con el objetivo de autenticarse con la red Wi-Fi. Esta configuración es válida únicamente si la opción "Tipo de autenticación" se establece en "SCEP". El nombre del perfil SCEP debe tener menos de 36 caracteres para los dispositivos que utilizan Knox Workspace.
Perfil de credenciales de usuario asociado	En esta configuración se especifica el perfil de credenciales de usuario asociado que utiliza un dispositivo con Android para obtener un certificado de cliente con el objetivo de autenticarse con la red Wi-Fi. Esta configuración es válida únicamente si la opción "Tipo de autenticación" se establece en "Credenciales del usuario". El nombre del perfil de credenciales de usuario debe tener menos de 36 caracteres para los dispositivos que utilizan Knox Workspace.
Nombre del certificado de cliente	En esta configuración se especifica el nombre del certificado de cliente que utiliza un dispositivo con Android para autenticarse con la red Wi-Fi. Esta configuración es válida únicamente si la opción "Tipo de vinculación de certificado" se establece en "Inyección variable".
Nombres comunes de certificado esperados por el servidor de autenticación	En la configuración se especifican los nombres comunes en el certificado que el servidor de autenticación debe enviar al dispositivo (por ejemplo, *.example.com). Esta configuración es válida únicamente si la opción "Tipo de seguridad" se establece en "Empresa".

Android: configuración del perfil de Wi-Fi	Descripción
Tipo de vinculación de certificado	En la configuración se especifica el tipo de vinculación para los certificados de confianza asociados al perfil de Wi-Fi. Esta configuración es válida únicamente si la opción "Tipo de seguridad" se establece en "Empresa". Valores posibles: • Referencia única • Inyección variable El valor predeterminado es "Referencia única".
Perfil de certificado de CA	En esta configuración se especifica el perfil de certificado de CA con el certificado de confianza que utiliza un dispositivo con Android para establecer una conexión de confianza con la red Wi-Fi. Esta configuración es válida únicamente si la opción "Tipo de vinculación de certificado" se establece en "Referencia única".
Nombres de certificados de confianza	En esta configuración se especifica los nombres de los certificados de confianza que utiliza un dispositivo con Android para establecer una conexión de confianza con la red Wi-Fi. Esta configuración es válida únicamente si la opción "Tipo de vinculación de certificado" se establece en "Inyección variable".

Windows: configuración del perfil de Wi-Fi

Windows: configuración del perfil de Wi-Fi	Descripción
Conectar automáticamente cuando esta red esté dentro del alcance	Esta configuración especifica si los dispositivos pueden conectarse automáticamente a la red Wi-Fi.
Tipo de seguridad	En la configuración se especifica el tipo de seguridad que utiliza la red Wi-Fi. Valores posibles: • Abierta • WPA-Enterprise • WPA-Personal • WPA2-Enterprise • WPA2-Personal El valor predeterminado es "Abierta".

Windows: configuración del perfil de Wi-Fi	Descripción
Tipo de cifrado	En la configuración se especifica el método de cifrado que utiliza la red Wi-Fi. La configuración "Tipo de seguridad" determina qué tipos de cifrado son compatibles y el valor predeterminado de esta configuración. Valores posibles: • Ninguno • WEP • TKIP • AES
Clave WEP	Esta configuración especifica la clave WEP para la red Wi-Fi. La clave WEP debe contener 10 o 26 caracteres hexadecimales (0-9, A-F) o bien 5 o 13 caracteres alfanuméricos (0-9, A-Z). Ejemplos de valores de clave hexadecimal son ABCDEF0123 o ABCDEF0123456789ABCDEF0123. Ejemplos de valores de clave alfanumérica son abCD5 o abCDefGHijKL1. Esta configuración solo es válida si la opción "Tipo de seguridad" se establece en "Abierta" y el "Tipo de cifrado" en "WEP".
Índice de clave	Esta configuración especifica la posición de la clave coincidente guardada en el punto de acceso inalámbrico. Esta configuración solo es válida si la opción "Tipo de seguridad" se establece en "Abierta" y el "Tipo de cifrado" en "WEP". Los valores posibles son de 1 a 4. El valor predeterminado es 2.
Clave compartida previamente	Esta configuración especifica la clave compartida previamente para la red Wi-Fi. Esta configuración es válida únicamente si la opción "Tipo de seguridad" se establece en "WPA-Personal".
Activar registro único	Esta configuración especifica si la red Wi-Fi es compatible con la autenticación de registro único. Esta configuración es válida únicamente si la opción "Tipo de seguridad" se establece en "WPA-Enterprise" o "WPA2-Enterprise".

Windows: configuración del perfil de Wi-Fi	Descripción
Tipo de registro único	Esta configuración especifica si se ha realizado la autenticación de registro único. Si se establece en "Realizar inmediatamente antes del inicio de sesión del usuario", se realizará el registro único antes de que el usuario inicie sesión en el directorio activo de la empresa. Si se establece en "Realizar inmediatamente después del inicio de sesión del usuario", se realizará el registro único inmediatamente después de que el usuario inicie sesión en el directorio activo de la empresa. Esta configuración solo es válida si se ha seleccionado la opción "Activar registro único". Valores posibles: • Realizar inmediatamente antes del inicio de sesión del usuario • Realizar inmediatamente después del inicio de sesión del usuario El valor predeterminado es "Realizar inmediatamente antes del inicio de sesión del usuario".
Retraso máximo de la conectividad	Esta configuración especifica, en segundos, la demora máxima antes de que falle el intento de conexión de registro único. Esta configuración solo es válida si se ha seleccionado la opción "Activar registro único". Los valores posibles son de 0 a 120 segundos. El valor predeterminado es de "10 segundos".
Permitir que se muestren diálogos adicionales durante el registro único	Esta configuración especifica si un dispositivo puede mostrar cuadros de diálogo a partir de la pantalla de inicio de sesión. Por ejemplo, si un tipo de autenticación EAP requiere que un usuario confirme el certificado enviado por el servidor durante la autenticación, el dispositivo podrá mostrar el cuadro de diálogo. Esta configuración solo es válida si se ha seleccionado la opción "Activar registro único".
Esta red utiliza LAN virtuales independientes para la autenticación de equipo y de usuario	Esta configuración especifica si la VLAN utilizada por un dispositivo cambia en función de la información de inicio de sesión del usuario. Por ejemplo, si el dispositivo se coloca en una VLAN cuando se inicia y, en función de los permisos de usuario, se transfiere a una red VLAN diferente después de que el usuario haya iniciado sesión. Esta configuración solo es válida si se ha seleccionado la opción "Activar registro único".
Validar certificado del servidor	Esta configuración especifica si un dispositivo debe validar el certificado de servidor que comprueba la identidad del punto de acceso inalámbrico. Esta configuración es válida únicamente si la opción "Tipo de seguridad" se establece en "WPA-Enterprise" o "WPA2-Enterprise".

Windows: configuración del perfil de Wi-Fi	Descripción
No solicitar al usuario que autorice nuevos servidores ni autoridades de certificación de confianza	Esta configuración especifica si se solicita a un usuario que confíe en el certificado de servidor. Esta configuración solo es válida si la opción "Validar certificado del servidor" está seleccionada.
Perfiles de certificado de CA	Esta configuración especifica el perfil del certificado de CA que proporciona la raíz de confianza del certificado de servidor que utiliza el punto de acceso inalámbrico. Esta configuración limita las CA raíz de las CA seleccionadas en la que confían los dispositivos. Si no se selecciona ninguna CA raíz de confianza, los dispositivos confiarán en todas las CA raíz incluidas en la lista de su almacén de autoridades de certificación raíz de confianza. Esta configuración solo es válida si la opción "Validar certificado del servidor" está seleccionada.
Activar reconexión rápida	Esta configuración especifica si la red Wi-Fi es compatible con la reconexión rápida para la autenticación PEAP a través de varios puntos de acceso inalámbricos. Esta configuración es válida únicamente si la opción "Tipo de seguridad" se establece en "WPA-Enterprise" o "WPA2-Enterprise".
Ejecutar NAP	Esta configuración especifica si la red Wi-Fi utiliza NAP para realizar comprobaciones de estado del sistema en los dispositivos para verificar que cumplan con los requisitos de salud antes de que se permitan las conexiones a la red. Esta configuración es válida únicamente si la opción "Tipo de seguridad" se establece en "WPA-Enterprise" o "WPA2-Enterprise".
Activar modo FIPS	Esta opción especifica si la red Wi-Fi es compatible con el cumplimiento del estándar FIPS 140-2. Esta configuración es válida únicamente si la opción "Tipo de seguridad" se establece en "WPA2-Enterprise" o "WPA2-Personal" y si la opción "Tipo de cifrado" se establece en "AES".
Activar almacenamiento en caché PMK	Esta configuración especifica si un dispositivo puede guardar la PMK para activar la roaming rápido de WPA2. La roaming rápida ignora los ajustes 802.1X gracias a un punto de acceso inalámbrico que se autenticó previamente en el dispositivo. Esta configuración solo es válida si la opción "Tipo de seguridad" se establece en "WPA2-Enterprise".

Windows: configuración del perfil de Wi-Fi	Descripción
Tiempo de PMK para activación	Esta configuración especifica el tiempo, en minutos, que un dispositivo puede guardar la PMK en caché. Esta configuración es válida únicamente si se ha seleccionado la opción "Permitir almacenamiento en caché PMK". Los valores posibles oscilan entre 5 y 1440 minutos. El valor predeterminado es de 720 minutos.
Número de entradas en la caché PMK	Esta configuración especifica el número máximo de entradas PMK que un dispositivo puede guardar en caché. Esta configuración es válida únicamente si se ha seleccionado la opción "Permitir almacenamiento en caché PMK". Los valores posibles son de 1 a 255. El valor predeterminado es 128.
Esta red utiliza la autenticación previa	Esta configuración especifica si el punto de acceso es compatible con la autenticación previa de la roaming rápida de WPA2. La autenticación previa permite que los dispositivos que se conectan a un punto de acceso inalámbrico realicen los ajustes 802.1X con otros puntos de acceso inalámbricos dentro de su alcance. La autenticación previa guarda la PMK y la información asociada en la caché PMK. Si el dispositivo se conecta a un punto de acceso inalámbrico con el que se ha autenticado previamente, se utilizará la información de PMK guardada para reducir el tiempo necesario de autenticación y conexión. Esta configuración es válida únicamente si se ha seleccionado la opción "Permitir almacenamiento en caché PMK".
Número máximo de intentos de autenticación previa	Esta configuración especifica el número máximo de intentos de autenticación previa permitido. Esta configuración solo es válida si la opción "Esta red utiliza la autenticación previa" está seleccionada. Los valores posibles son de 1 a 16. El valor predeterminado es 3.
Tipo de proxy	Esta configuración especifica el tipo de configuración de proxy para el perfil Wi-Fi. Configuración posible: • Ninguno • Configuración de PAC • Configuración manual • Autodetección de proxy web La configuración predefinida es "Configuración manual". La configuración se aplica únicamente a dispositivos Windows 10 Mobile.

Windows: configuración del perfil de Wi-Fi	Descripción
URL de PAC	En la configuración se especifica la URL del servidor web que aloja el archivo de PAC y el nombre del archivo en formato http://<web_server_URL>/<filename>.pac. Esta configuración es válida únicamente si la opción "Tipo de proxy" se establece en "Configuración de PAC".
Dirección	Esta configuración especifica el nombre del servidor y el puerto de la red proxy. Utilice el formato host:puerto (por ejemplo, server01.example.com:123). El host debe ser uno de los siguientes: • Un nombre registrado, como un nombre de servidor, FQDN o nombre de una sola etiqueta (por ejemplo, server01 en lugar de server01.example.com) • Una dirección IPv4 o IPv6 Esta configuración es válida únicamente si la opción "Tipo de proxy" se establece en "Configuración manual".
Autodetección de proxy web	En la configuración se especifica si desea activar el Protocolo de autodescubrimiento de proxy web (WPAD) para la búsqueda de proxy. Esta configuración es válida únicamente si la opción "Tipo de proxy" se establece en "Autodetección de proxy web". De forma predeterminada, esta casilla de verificación no está activada.
Desactivar comprobaciones de conectividad a Internet	En la configuración se especifica si desea desactivar las comprobaciones de conectividad a Internet. De forma predeterminada, esta casilla de verificación no está activada.
Perfil SCEP asociado	En la configuración se especifica el perfil SCEP asociado que un dispositivo debe utilizar para obtener un certificado de cliente con el objetivo de autenticarlo con la red Wi-Fi.

Configuración de las VPN de trabajo para dispositivos

Puede utilizar un perfil de VPN para especificar cómo los dispositivos con iOS, iPadOS, macOS, Samsung Knox y Windows 10 se conectan a una VPN de trabajo. Se puede asignar un perfil de VPN a cuentas de usuarios, a grupos de usuarios y a grupos de dispositivos.

Para conectar una VPN de trabajo para dispositivos Android que no sean Samsung Knox, puede configurar ajustes de VPN utilizando los ajustes de configuración de la aplicación para una aplicación VPN o los usuarios pueden configurar manualmente los ajustes de VPN en sus dispositivos.

Dispositivo	Aplicaciones y conexiones de red
iOS y iPadOS	Tanto las aplicaciones de trabajo como las personales pueden utilizar los perfiles VPN guardados en el dispositivo para conectarse a la red de la empresa. Puede activar una VPN por aplicación para que un perfil de VPN limite el perfil de las aplicaciones de trabajo que se especifiquen. Puede activar VPN a petición para que los dispositivos se conectan automáticamente a una VPN en un dominio particular. Por ejemplo, puede especificar el dominio de la empresa para que los usuarios puedan acceder al contenido de su intranet mediante una VPN a petición.
macOS	Puede configurar perfiles de VPN para permitir que las aplicaciones se conecten a la red de la empresa. Puede activar VPN a petición para que los dispositivos se conectan automáticamente a una VPN en un dominio particular. Por ejemplo, puede especificar el dominio de la empresa para que los usuarios puedan acceder al contenido de su intranet mediante una VPN a petición.
Samsung Knox	En los dispositivos con Samsung Knox con activaciones de Android Enterprise o Samsung Knox Workspace, las aplicaciones de trabajo pueden utilizar los perfiles VPN guardados en el dispositivo para conectarse a la red de la empresa. Puede activar una VPN por aplicación para limitar el perfil de las aplicaciones de trabajo que se especifiquen. Una aplicación de cliente VPN compatible debe estar instalada en el dispositivo. Cisco AnyConnect y Juniper son compatibles. **Nota:** La aplicación Juniper solo es compatible con SSL VPN.
Windows 10	Puede configurar perfiles de VPN para permitir que las aplicaciones se conecten a la red de la empresa. En el perfil de VPN, puede especificar una lista de aplicaciones que debe utilizar la VPN.

Crear un perfil VPN

Puede utilizar CylanceGATEWAY para crear un perfil de acceso a la red de confianza cero (ZTNA) reconocido por los dispositivos como un proveedor de VPN. CylanceGATEWAY no confía en nada ni en nadie de manera predeterminada. Para obtener más información sobre CylanceGATEWAY, consulte Integración de BlackBerry UEM con CylanceGATEWAY para crear un perfil ZTNA.

La configuración del perfil obligatorio varía para cada tipo de dispositivo y depende del tipo de conexión VPN y del tipo de autenticación que seleccione.

Nota: Algunos dispositivos pueden no ser capaces de guardar la contraseña xAuth. Para obtener más información, visite support.blackberry.com/community para leer el artículo 30353.

Antes de empezar:

- Si los dispositivos utilizan la autenticación basada en certificados para conexiones VPN de trabajo, cree un perfil de certificado de CA y asígnelo a las cuentas de usuario, a los grupos de usuarios o a los grupos de dispositivos. Para enviar certificados de cliente a dispositivos, cree un perfil de credenciales de usuario, SCEP o certificado compartido para asociarlo al perfil de VPN.
- Para los dispositivos con iOS, iPadOS, macOS y Samsung Knox que utilizan un servidor proxy, cree un perfil de proxy para asociarlo al perfil de VPN. (El servidor proxy para los dispositivos con Windows 10 se configura en el perfil de VPN).
- Para dispositivos con Samsung Knox, agregue la aplicación de cliente VPN apropiada a la lista de aplicaciones y asígnela a las cuentas de usuario, a los grupos de usuarios o a los grupos de dispositivos. Las aplicaciones de cliente VPN admitidas son Cisco AnyConnect y Juniper.

1. En la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Redes y conexiones > VPN**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil VPN. Dicha información se muestra en los dispositivos.
5. Realice las acciones siguientes:
   a) Haga clic en la pestaña de un tipo de dispositivo.
   b) Configure los valores adecuados para cada configuración del perfil para que coincidan con la configuración de la red VPN del entorno de la empresa. Si la empresa requiere que los usuarios proporcionen un nombre de usuario y una contraseña para conectarse a la VPN y el perfil es para varios usuarios, en el campo **Nombre de usuario** escriba `%UserName%`.
6. Repita el paso 5 para cada tipo de dispositivo en la empresa.
7. Haga clic en **Agregar**.

Integración de BlackBerry UEM con CylanceGATEWAY para crear un perfil ZTNA

CylanceGATEWAY es una solución de acceso a la red de confianza cero (ZTNA) asistida por inteligencia artificial (IA) nativa de la nube. Cuando CylanceGATEWAY se activa en un dispositivo, se crea un perfil ZTNA que el dispositivo reconoce como proveedor VPN. CylanceGATEWAY no confía en nada ni en nadie de manera predeterminada.

- CylanceGATEWAY protege los dispositivos iOS, Android, Windows 10, Windows 11 y macOS permitiéndole bloquear las conexiones a destinos de Internet con los que no desea que contacten los dispositivos, incluso cuando el dispositivo no está conectado a la red.
- Además de proteger los dispositivos, CylanceGATEWAY protege el acceso a la red privada de su empresa y a las aplicaciones basadas en la nube mediante el análisis continuo de los patrones de uso de los usuarios para comprobar si son comportamientos esperados o anómalos. Si el porcentaje de eventos anómalos supera un umbral establecido, CylanceGATEWAY puede anular dinámicamente la política de control de acceso a la red del usuario para bloquear el acceso a la red y requerir que el usuario se autentique antes de continuar.

Los administradores de CylanceGATEWAY pueden configurar los destinos de Internet y de red privada a los que los usuarios pueden acceder o bloquear el acceso.

Para obtener más información sobre cómo configurar CylanceGATEWAY, consulte Configuración de BlackBerry Gateway en el contenido de configuración de Cylance Endpoint Security.

Configuración de perfil VPN

Puede utilizar una variable en cualquier ajuste de perfil que sea un campo de texto para hacer referencia a un valor en lugar de especificar el valor real. Los perfiles de VPN son compatibles con los siguientes tipos de dispositivos:

- iOS
- iPadOS
- macOS
- Samsung Knox
- Windows 10

iOS y macOS: Configuración de perfil VPN

La configuración para iOS también se aplica a los dispositivos con iPadOS.

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

iOS y macOS: Configuración de perfil VPN	Descripción
Aplicar perfil a	Esta configuración especifica si el perfil VPN de un dispositivo macOS se aplica a la cuenta de usuario o al dispositivo. Valores posibles: • Usuario • Dispositivo Esta configuración solo es válida para dispositivos macOS.

iOS y macOS: Configuración de perfil VPN	Descripción
Tipo de conexión	Esta configuración especifica el tipo de conexión que un dispositivo debe utilizar para una puerta de enlace VPN. Algunos tipos de conexión también requieren que los usuarios instalen la aplicación de VPN correspondiente en el dispositivo. Valores posibles: • L2TP • PPTP • IPsec • Cisco AnyConnect • Juniper • Pulse Secure • F5 • SonicWALL Mobile Connect • Aruba VIA • Check Point Mobile • OpenVPN • Personalizada • IKEv2 • IKEv2 siempre activado El valor predeterminado es "L2TP". Si selecciona "IKEv2 siempre activado", muchos ajustes tienen valores separados para conexiones de telefonía móvil y Wi-Fi. Algunos valores no son válidos para los dispositivos con macOS.
ID de paquete de VPN	Esta configuración especifica el ID de paquete de la aplicación VPN para una SSL VPN personalizada. El ID de paquete se muestra en formato DNS inverso (por ejemplo, com.ejemplo.VPNapp). Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "Personalizar".
Servidor	Dicha configuración especifica las direcciones FQDN o IP del servidor VPN.
Nombre de usuario	Esta configuración especifica el nombre de usuario que un dispositivo debe utilizar para autenticar con la puerta de enlace VPN. Si el perfil es para varios usuarios, puede especificar la variable %UserName%.
Pares clave-valor personalizados	Esta configuración especifica las claves y los valores asociados de la SSL VPN personalizada. La información de configuración es específica de la aplicación VPN del proveedor. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "Personalizar".

iOS y macOS: Configuración de perfil VPN	Descripción
Dominio o grupo de inicio de sesión	En la configuración se especifica el dominio o grupo de inicio de sesión que la puerta de enlace VPN debe utilizar para autenticar un dispositivo. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "SonicWALL Mobile Connect".
Alcance	En la configuración se especifica el nombre del dominio de autenticación que la puerta de enlace VPN debe utilizar para autenticar un dispositivo. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "Juniper" o "Pulse Secure."
Cargo	En la configuración se especifica el nombre de la función de usuario que la puerta de enlace VPN debe utilizar para verificar los recursos de red a los que puede acceder un dispositivo. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "Juniper" o Pulse Secure."
Tipo de autenticación	Esta configuración especifica el tipo de autenticación para la puerta de enlace VPN. La configuración "Tipo de conexión" determina qué tipos de autenticación son compatibles y el valor predeterminado para esta configuración. Valores posibles: • Contraseña • RSA SecurID • Secreto compartido • Secreto compartido/Nombre del grupo • Certificado compartido • SCEP • Credencial de usuario
Complementos de EAP	Esta configuración especifica el método de autenticación para la VPN. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "L2TP" o "PPTP" y la opción "Tipo de autenticación" se establece en "RSA SecurID".
Protocolo de autenticación	Esta configuración especifica los protocolos de autenticación para la VPN. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "L2TP" o "PPTP" y la opción "Tipo de autenticación" se establece en "RSA SecurID".
Contraseña	Esta configuración especifica la contraseña que un dispositivo debe utilizar para autenticar con la puerta de enlace VPN. Esta configuración es válida únicamente si la opción "Tipo de autenticación" se establece en "Contraseña".

iOS y macOS: Configuración de perfil VPN	Descripción
Nombre del grupo	Esta configuración especifica el nombre del grupo para la puerta de enlace VPN. Este ajuste es válido únicamente en las siguientes condiciones: • El ajuste "Tipo de conexión" se establece en "Cisco AnyConnect". • El ajuste "Tipo de conexión" se establece en "IPsec" y el ajuste "Tipo de autenticación" se establece en "Secreto compartido/Nombre del grupo".
Secreto compartido	Esta configuración especifica el secreto compartido que se utiliza para la autenticación VPN. Este ajuste es válido únicamente en las siguientes condiciones: • El ajuste "Tipo de conexión" se establece en "L2TP". • El ajuste "Tipo de conexión" se establece en "IPsec" y el ajuste "Tipo de autenticación" se establece en "Secreto compartido/Nombre del grupo". • El ajuste "Tipo de conexión" se establece en "IKEv2" o "IKEv2 siempre activado" y el "Método de autenticación" se establece en "Secreto compartido".
Perfil de certificado compartido	Esta configuración especifica el perfil de certificado compartido con el certificado de cliente que un dispositivo debe utilizar para autenticar con la puerta de enlace VPN. Esta configuración es válida únicamente si la opción "Tipo de autenticación" se establece en "Certificado compartido".
Perfil SCEP asociado	En la configuración se especifica el perfil SCEP asociado que un dispositivo debe utilizar para obtener un certificado de cliente con el objetivo de autenticarlo con la VPN. Esta configuración es válida únicamente si la opción "Tipo de autenticación" se establece en "SCEP".
Perfil de credenciales de usuario asociado	Esta configuración especifica el perfil de credenciales de usuario asociado que un dispositivo debe utilizar para obtener un certificado de cliente con el objetivo de autenticarlo con la red VPN. Esta configuración es válida únicamente si la opción "Tipo de autenticación" se establece en "Credenciales del usuario".

iOS y macOS: Configuración de perfil VPN	Descripción
Nivel de cifrado	Esta configuración especifica el nivel de cifrado de datos de la conexión VPN. Si la configuración se establece en "Automática", se permite el uso de todas las intensidades de cifrado disponibles. Si la configuración se establece en "Máxima", solo se permitirá la intensidad de cifrado máxima. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "PPTP". Valores posibles: • Ninguno • Automático • Máximo El valor predeterminado es "Ninguno".
Enrutar tráfico de red a través de VPN	Esta configuración especifica si se enviará todo el tráfico de red a través de la conexión VPN. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "L2TP" o "PPTP".
Usar autenticación híbrida	Esta configuración especifica si se utilizará un certificado de servidor para la autenticación. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "IPsec" y el "Tipo de autenticación" se establece en "Secreto compartido/Nombre del grupo"
Solicitar contraseña	Esta configuración especifica si un dispositivo debe solicitar una contraseña al usuario. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "IPsec" y el "Tipo de autenticación" se establece en "Secreto compartido/Nombre del grupo"
Solicitar PIN de usuario	Esta configuración especifica si el dispositivo debe solicitar un PIN al usuario. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "IPsec" y la opción "Tipo de autenticación" se establece en "Certificado compartido", en "SCEP" o en "Credenciales del usuario".
Dirección remota	Esta configuración especifica las direcciones IP o el nombre de host del servidor VPN. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "IKEv2" o "IKEv2 siempre activado".
ID local	Esta configuración especifica la identidad del cliente IKEv2 en uno de los siguientes formatos: FQDN, FQDN de usuario, Dirección y ASN1DN. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "IKEv2" o "IKEv2 siempre activado".

iOS y macOS: Configuración de perfil VPN	Descripción
ID remoto	Esta configuración especifica el identificador remoto del cliente IKEv2 con uno de los formatos siguientes: FQDN, FQDN de usuario, Dirección o ASN1DN. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "IKEv2" o "IKEv2 siempre activado".
Activar VPN a petición	Esta configuración especifica si un dispositivo puede iniciar automáticamente una conexión VPN al acceder a determinados dominios. En dispositivos con iOS y iPadOS, esta configuración se aplica a las aplicaciones de trabajo. Este ajuste es válido únicamente en las siguientes condiciones: • El ajuste "Tipo de conexión" se establece en "IPsec", "Cisco AnyConnect," "Juniper", "Pulse Secure", "F5", "SonicWALL Mobile Connect", "Aruba VIA", "Check Point Mobile", "OpenVPN" o "Personalizada" y el ajuste "Tipo de autenticación" se establece en "Certificado compartido", en "SCEP" o en "Credenciales del usuario". • El ajuste "Tipo de conexión" se establece en "IKEv2" y el "Método de autenticación" se establece en "Certificado compartido".
Nombres de host o dominio que pueden usar VPN a petición	Esta configuración especifica los dominios y las acciones asociadas a VPN a petición. Esta configuración es válida únicamente si se ha seleccionado la opción "Activar VPN a petición". Los valores posibles para "Acción a petición": • Establecer siempre • Establecer si es necesario • No establecer nunca
Reglas de VPN a petición para iOS 7.0 y posteriores	Esta configuración especifica los requisitos de la conexión para VPN a petición. Debe utilizar una o más claves del ejemplo de formato de carga. La configuración anula el ajuste "Nombres de host o dominio que pueden usar VPN a petición". Esta configuración es válida únicamente si se ha seleccionado la opción "Activar VPN a petición".
Desconectar por inactividad	Esta configuración especifica si la conexión VPN debe desconectarse cuando esté inactiva durante un periodo de tiempo determinado. Esta configuración es válida únicamente si se ha seleccionado la opción "Activar VPN a petición".

iOS y macOS: Configuración de perfil VPN	Descripción
Desconectar por inactividad del temporizador	Esta configuración especifica el tiempo de inactividad en segundos tras el que debe desconectarse la VPN. El valor predeterminado es "120". Esta configuración es válida únicamente si se ha seleccionado la opción "Desconectar por inactividad".
No permitir que el usuario desactive la VPN a petición	Esta configuración especifica si el usuario puede desactivar la VPN a petición. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "IPsec", "Cisco AnyConnect", "Juniper", "Pulse Secure", "F5", "SonicWALL Mobile Connect", "Aruba VIA", "Check Point Mobile", "OpenVPN" o "Personalizar". Esta configuración se aplica únicamente a los dispositivos que ejecutan iOS y iPadOS 14 y posteriores.
Excluir red local	Esta configuración especifica si se debe excluir el tráfico de red local de la conexión VPN. Si también está seleccionada la opción "Incluir todas las redes", no se enrutará ningún tráfico de red local a través de la VPN. Esta configuración se aplica únicamente a los dispositivos que ejecutan iOS y iPadOS 13 y posteriores.
Todas las rutas no predeterminadas tienen prioridad sobre cualquier ruta definida localmente	En la configuración se especifica si las rutas no predeterminadas de la VPN tienen prioridad sobre cualquier ruta definida localmente. Si también se selecciona el ajuste “Incluir todas las redes”, este ajuste se ignora. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "Cisco AnyConnect", "Juniper", "Pulse Secure", "F5", "SonicWALL Mobile Connect", "Aruba VIA", "Check Point Mobile", "OpenVPN" o "Personalizar". Esta configuración se aplica únicamente a los dispositivos que ejecutan iOS y iPadOS 14,2 y posteriores.
Incluir todas las redes	Esta configuración especifica si todo el tráfico de red debe enrutarse a través de la conexión VPN. Si también se selecciona "Excluir red local", el tráfico de red local no se enrutará a través de la VPN. Esta configuración se aplica únicamente a los dispositivos que ejecutan iOS y iPadOS 13 y posteriores.
Requisito designado por el proveedor	Esta configuración especifica un proveedor de VPN designado. Si el proveedor de VPN se implementa como una extensión del sistema, esta configuración es obligatoria. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "IPsec", "Cisco AnyConnect", "Juniper", "Pulse Secure", "F5", "SonicWALL Mobile Connect", "Aruba VIA", "Check Point Mobile", "OpenVPN" o "Personalizar".

iOS y macOS: Configuración de perfil VPN	Descripción
Permitir que el usuario desactive la conexión automática	Esta configuración especifica si los usuarios pueden desactivar la conexión VPN. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "IKEv2 siempre activado".
Utilizar la misma configuración de túnel para el uso de la red móvil y Wi-Fi	Esta configuración especifica si desea establecer una configuración de VPN individual para el dispositivo en función de que este vaya a enviar datos a través de una red móvil o una red Wi-Fi. Si no se selecciona esta opción, puede definir diferentes ajustes de red móvil y Wi-Fi en el mismo perfil. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "IKEv2 siempre activado".
Activar xAuth	Esta configuración especifica si la VPN es compatible con la autenticación extendida. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "IKEv2" o "IKEv2 siempre activado".
Versión mínima de TLS	Esta configuración especifica la versión mínima de TLS que los dispositivos utilizan para la autenticación EAP-TLS. Esta configuración es válida únicamente si se selecciona la opción "Activar xAuth" y el Tipo de autenticación es "Certificado". Valores posibles: • 1,0 • 1,1 • 1,2 La configuración predeterminada es "1.0".
Versión máxima de TLS	Esta configuración especifica la versión máxima de TLS que los dispositivos utilizan para la autenticación EAP-TLS. Esta configuración es válida únicamente si se selecciona la opción "Activar xAuth" y el Tipo de autenticación es "Certificado". Valores posibles: • 1,0 • 1,1 • 1,2 La configuración predeterminada es "1.2".
Tipo de certificado	En la configuración se especifica el tipo de certificado utilizado para la autenticación de equipo IKEv2. Esta configuración es válida únicamente si se selecciona la opción "Activar xAuth" y el Tipo de autenticación es "Certificado".

iOS y macOS: Configuración de perfil VPN	Descripción
Nombre común del emisor del certificado de servidor	Esta configuración especifica el nombre común del CA que emitió el certificado del servidor que el servidor IKE debe enviar al dispositivo. Si activa xAuth mediante un certificado, esta configuración es obligatoria. Esta configuración es válida únicamente si se selecciona la opción "Activar xAuth" y el Tipo de autenticación es "Certificado".
Nombre común del certificado de servidor	Esta configuración especifica el nombre común del certificado del servidor que el servidor IKE debe enviar al dispositivo. Esta configuración es válida únicamente si se selecciona la opción "Activar xAuth" y el Tipo de autenticación es "Certificado".
Intervalo de Keepalive	Esta configuración especifica la frecuencia con la que un dispositivo envía un paquete Keepalive. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "IKEv2" o "IKEv2 siempre activado". Valores posibles: • Desactivado • 30 minutos • 10 minutos • 1 minuto La configuración predeterminada es "10 minutos".
Desactivar MOBIKE	Esta configuración especifica si MOBIKE está desactivado. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "IKEv2" o "IKEv2 siempre activado".
Desactivar redirección de IKEv2	Esta configuración especifica si la redirección de IKEv2 está desactivada. Si la configuración no está seleccionada, la conexión IKEv2 se redirecciona si se recibe una solicitud de redirección del servidor. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "IKEv2" o "IKEv2 siempre activado".
Activar confidencialidad directa total	Esta configuración especifica si la puerta de enlace VPN debe ser compatible con PFS. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "IKEv2" o "IKEv2 siempre activado".
Activar NAT Keepalive	Esta configuración especifica si la puerta de enlace VPN debe ser compatible con paquetes de NAT Keepalive. Los paquetes Keepalive se utilizan para mantener las asignaciones NAT para conexiones IKEv2. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "IKEv2" o "IKEv2 siempre activado".

iOS y macOS: Configuración de perfil VPN	Descripción
Intervalo de NAT Keepalive	Esta configuración especifica la frecuencia con la que un dispositivo envía un paquete de NAT Keepalive (en segundos). Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "IKEv2" o "IKEv2 siempre activo" y si se selecciona la opción "Activar NAT Keepalive". El valor mínimo y el valor predeterminado son 20.
Usar subredes internas IKEv2 IPv4 e IPv6	Esta configuración especifica si la VPN puede utilizar los atributos de configuración IKEv2 INTERNAL_IP4_SUBNET e INTERNAL_IP6_SUBNET. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "IKEv2" o "IKEv2 siempre activado".
Nombre común del certificado de servidor	Esta configuración especifica el nombre común en el certificado que el servidor IKE debe enviar al dispositivo. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "IKEv2" o "IKEv2 siempre activado".
Nombre común del emisor del certificado de servidor	Esta configuración especifica el nombre común del emisor del certificado en el certificado que el servidor IKE debe enviar al dispositivo. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "IKEv2" o "IKEv2 siempre activado".
Activar comprobación de revocación de certificado	Esta configuración especifica si se intenta realizar una comprobación de revocación de certificado para el certificado del servidor. La comprobación no fallará si no hay respuesta. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "IKEv2" o "IKEv2 siempre activado".
Activar reserva	Esta configuración especifica si el dispositivo puede establecer un túnel VPN a través de la red móvil cuando Wi-Fi Assist está activado. Esta configuración se aplica solo a dispositivos que ejecutan iOS y iPadOS 13 y posteriores, y requiere que el servidor admita varios túneles para usuarios individuales. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "IKEv2" o "IKEv2 siempre activado".
Aplicar parámetros de asociación de seguridad secundarios	Esta configuración especifica si desea aplicar parámetros de asociación de seguridad secundarios. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "IKEv2" o "IKEv2 siempre activado".
Aplicar parámetros de asociación de seguridad IKE	Esta configuración especifica si desea aplicar parámetros de asociación de seguridad IKE. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "IKEv2" o "IKEv2 siempre activado".

iOS y macOS: Configuración de perfil VPN	Descripción
MTU	Esta configuración especifica la Unidad de transmisión máxima en bytes. Esta configuración se aplica únicamente a los dispositivos que ejecutan iOS y iPadOS 14 y posteriores. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "IKEv2 siempre activado".
Mensaje de voz	Este ajuste especifica si las conexiones al servicio de correo de voz se envían a través del túnel VPN, se envían fuera del túnel VPN o se bloquean. Esta configuración se aplica únicamente a los dispositivos que ejecutan iOS y iPadOS 13,4 y posteriores. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "IKEv2 siempre activado". Solo se aplica a las conexiones Wi-Fi.
AirPrint	Esta configuración especifica si las conexiones AirPrint AirPrint se envían a través del túnel VPN, se envían fuera del túnel VPN o se bloquean. Esta configuración se aplica únicamente a los dispositivos que ejecutan iOS y iPadOS 13,4 y posteriores. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "IKEv2 siempre activado". Solo se aplica a las conexiones Wi-Fi.
Permitir el tráfico desde hojas de redes cautivas fuera del túnel VPN	Esta configuración se especifica si el tráfico de las hojas de redes cautivas se puede enviar fuera del túnel VPN. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "IKEv2 siempre activado". Solo se aplica a las conexiones Wi-Fi.
Permitir el tráfico desde todas las aplicaciones de redes cautivas fuera del túnel VPN	Esta configuración se especifica si el tráfico de todas las aplicaciones de redes cautivas puede enviarse fuera del túnel VPN. Si no se selecciona esta opción, puede especificar aplicaciones individuales para las que se puede enviar tráfico fuera del túnel. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "IKEv2 siempre activado". Solo se aplica a las conexiones Wi-Fi.
Se permite el tráfico desde estas aplicaciones fuera del túnel VPN	En la configuración se especifican las aplicaciones de redes cautivas individuales para las que se puede enviar tráfico fuera del túnel. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "IKEv2 siempre activado". Solo se aplica a las conexiones Wi-Fi.
Permitir el tráfico de aplicaciones fuera del túnel VPN	En la configuración se especifican las aplicaciones cuyo tráfico se puede enviar fuera del túnel. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "IKEv2 siempre activado". Solo se aplica a las conexiones Wi-Fi.

iOS y macOS: Configuración de perfil VPN	Descripción
Grupo DH	Esta configuración especifica el grupo DH que un dispositivo utiliza para generar el material de clave. Esta configuración es válida únicamente si la opción "Aplicar parámetros de asociación de seguridad secundarios" o "Aplicar parámetros de asociación de seguridad IKE" está seleccionada. Valores posibles: • 0 • 1 • 2 • 5 • 14 • 15 • 16 • 17 • 18 • 19 • 20 • 21 • 31 La configuración predeterminada es "2".
Algoritmo de cifrado	Esta configuración especifica el algoritmo de cifrado IKE. Esta configuración es válida únicamente si la opción "Aplicar parámetros de asociación de seguridad secundarios" o "Aplicar parámetros de asociación de seguridad IKE" está seleccionada. Valores posibles: • DES • 3DES • AES 128 • AES 256 • AES 128 GCM • AES 256 GCM • Artículo ChaCha20Poly1305 La configuración predeterminada es "3DES".

iOS y macOS: Configuración de perfil VPN	Descripción
Algoritmo de integridad	Esta configuración especifica el algoritmo de integridad IKE. Esta configuración es válida únicamente si la opción "Aplicar parámetros de asociación de seguridad secundarios" o "Aplicar parámetros de asociación de seguridad IKE" está seleccionada. Valores posibles: • SHA1 96 • SHA1 160 • SHA1 256 • SHA2 384 • SHA2 512 El valor predeterminado es "SHA1-96".
Intervalo para regenerar claves	Esta configuración especifica la duración de la conexión IKE. Esta configuración es válida únicamente si la opción "Aplicar parámetros de asociación de seguridad secundarios" o "Aplicar parámetros de asociación de seguridad IKE" está seleccionada. Los valores posibles son de 10 a 1440 minutos. El valor predeterminado es 1440.
Activar VPN por aplicación	Esta configuración especifica si la puerta de enlace VPN debe ser compatible con VPN por aplicación. Esta característica ayuda a disminuir la carga sobre una VPN de la empresa. Por ejemplo, puede activar que solo un determinado tráfico de trabajo utilice la VPN, por ejemplo, al acceder a servidores de aplicaciones o páginas web detrás del firewall. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "Cisco AnyConnect", "Juniper", "Pulse Secure", "F5", "SonicWALL Mobile Connect", "Aruba VIA", "Check Point Mobile", "OpenVPN", "Personalizar", "IKEv2" o "IKEv2 siempre activado".
Permitir la conexión automática de aplicaciones	Esta configuración especifica si las aplicaciones asociadas a VPN por aplicación pueden iniciar automáticamente la conexión VPN. Esta configuración es válida únicamente si se ha seleccionado la opción "Activar VPN por aplicación".
Dominios de Safari	Esta configuración especifica el dominio que puede iniciar la conexión VPN en Safari. Esta configuración es válida únicamente si se ha seleccionado la opción "Activar VPN por aplicación".

iOS y macOS: Configuración de perfil VPN	Descripción
Dominios de calendario	Esta configuración especifica los dominios que pueden iniciar la conexión VPN en Calendario. Esta configuración es válida únicamente si se ha seleccionado la opción "Activar VPN por aplicación". Esta configuración se aplica únicamente a dispositivos que ejecutan iOS y iPadOS 13.0 y posteriores.
Dominios de contactos	Esta configuración especifica los dominios que pueden iniciar la conexión VPN en Contactos. Esta configuración es válida únicamente si se ha seleccionado la opción "Activar VPN por aplicación". Esta configuración se aplica únicamente a dispositivos que ejecutan iOS y iPadOS 13.0 y posteriores.
Dominios de correo	Esta configuración especifica los dominios que pueden iniciar la conexión VPN en Correo. Esta configuración es válida únicamente si se ha seleccionado la opción "Activar VPN por aplicación". Esta configuración se aplica únicamente a dispositivos que ejecutan iOS y iPadOS 13.0 y posteriores.
Dominios asociados	Esta configuración especifica el dominio que puede iniciar la conexión VPN en el dispositivo. Los dominios también deben incluirse en el archivo apple-app-site-association. Esta configuración es válida únicamente si se ha seleccionado la opción "Activar VPN por aplicación". Esta configuración se aplica únicamente a dispositivos que ejecutan iOS y iPadOS 14.0 y posteriores.
Dominios excluidos	Esta configuración especifica que los dominios que están bloqueados no pueden iniciar la conexión VPN en el dispositivo. Esta configuración es válida únicamente si se ha seleccionado la opción "Activar VPN por aplicación". Esta configuración se aplica únicamente a dispositivos que ejecutan iOS y iPadOS 14.0 y posteriores.
Tunelización de tráfico	Esta configuración especifica si la VPN tuneliza el tráfico en la capa de aplicación o la capa IP. Esta configuración es válida únicamente si se ha seleccionado la opción "Activar VPN por aplicación". Esta configuración se aplica únicamente a dispositivos que ejecutan iOS y iPadOS 13.0 y posteriores. Valores posibles: • Capa de aplicación • Capa IP La configuración predeterminada es "Capa de aplicación".
Perfil proxy asociado	Esta configuración especifica el perfil de proxy asociado que un dispositivo debe utilizar para conectarse al servidor proxy cuando el dispositivo está conectado a la red VPN.

Android: configuración del perfil de VPN

Las siguientes configuraciones del perfil VPN solo son compatibles con dispositivos Samsung Knox Workspace.

Para obtener más información sobre las configuración de perfil VPN compatibles con los dispositivos Samsung Knox Workspace, consulte Parámetros JSON VPN de Samsung Knox.

Android: configuración del perfil de VPN	Descripción
Dirección de servidor	Dicha configuración especifica las direcciones FQDN o IP del servidor VPN.
Tipo de VPN	En la configuración se especifica si el dispositivo debe utilizar IPsec o SSL para conectarse al servidor VPN. Valores posibles: • IPsec • SSL El valor predeterminado es "IPsec". La aplicación VPN de Juniper solo admite "SSL".
Autenticación de usuario requerida	En la configuración se especifica si un usuario del dispositivo debe proporcionar un nombre de usuario y una contraseña para conectarse al servidor VPN.
Nombre de usuario	Esta configuración especifica el nombre de usuario que un dispositivo debe utilizar para autenticar con la puerta de enlace VPN. Si el perfil es para varios usuarios, puede utilizar la variable %UserName%. Esta configuración es válida únicamente si se ha seleccionado la opción "Autenticación de usuario requerida".
Contraseña	Esta configuración especifica la contraseña que un dispositivo debe utilizar para autenticar con la puerta de enlace VPN. Esta configuración es válida únicamente si se ha seleccionado la opción "Autenticación de usuario requerida".
Tipo de túnel dividido	En la configuración se especifica si un dispositivo puede usar la tunelización dividida para omitir la puerta de enlace VPN, siempre que esta la admita. Valores posibles: • Desactivado • Manual • Automático Si el ajuste "Tipo de VPN" se establece en "IPsec", este ajuste se debe establecer en "Desactivado". El valor predeterminado es "Desactivado".
Rutas de reenvío	En la configuración se especifica la ruta o rutas que omiten la puerta de enlace VPN. Puede especificar una o más direcciones IP. La configuración es válida únicamente si el ajuste "Tipo de VPN" se establece en "SSL" y el ajuste "Tipo de túnel dividido" se establece en "Manual".

Android: configuración del perfil de VPN	Descripción
DPD	En la configuración se especifica si DPD está activado. Esta configuración es válida únicamente si la opción "Tipo de VPN" se establece en "IPsec".
Versión de IKE	En la configuración especifica la versión del protocolo IKE que debe utilizar con la conexión VPN. Valores posibles: • IKEv1 • IKEv2 El valor predeterminado es "IKEv1". Esta configuración es válida únicamente si la opción "Tipo de VPN" se establece en "IPsec".
Tipo de autenticación IPsec	En la configuración se especifica el tipo de autenticación para la conexión VPN IPsec. La configuración "Versión de IKE" determina qué tipos de autenticación IPsec son compatibles y el valor predeterminado para esta configuración. Valores posibles: • Certificado • Clave compartida previamente • EAP MD5 • EAP MSCHAPv2 • RSA híbrida • Autenticación basada en CAC Esta configuración es válida únicamente si la opción "Tipo de VPN" se establece en "IPsec".
Tipo de ID de grupo IPsec	En la configuración se especifica el tipo de ID de grupo IPsec para VPN. La configuración "Tipo de autenticación IPsec" determina qué tipos de ID de grupo IPsec son compatibles y el valor predeterminado para esta configuración. Valores posibles: • Predeterminado • Dirección IPv4 • Nombre de dominio completo • FQDN de usuario • ID de clave IKE Si la configuración de "Tipo de autenticación IPsec" es "Certificado", la configuración se establece automáticamente en "Predeterminada". Esta configuración es válida únicamente si la opción "Tipo de VPN" se establece en "IPsec".

Android: configuración del perfil de VPN	Descripción
ID de grupo IPsec	En la configuración se especifica el ID de grupo IPsec para VPN. Esta configuración es válida únicamente si la opción "Tipo de VPN" se establece en "IPsec".
Modo de intercambio de clave IKE fase 1	En la configuración se especifica el modo de intercambio para VPN. Valores posibles: • Modo principal • Modo agresivo El valor predeterminado es "Modo principal". Esta configuración es válida únicamente si la opción "Tipo de VPN" se establece en "IPsec".
Duración de IKE	En la configuración se especifica la duración, en segundos, de la conexión IKE. Si establece un valor no admitido o un valor nulo, se usará el valor predeterminado del dispositivo. Esta configuración es válida únicamente si la opción "Tipo de VPN" se establece en "IPsec".
Algoritmo de cifrado IKE	En la configuración se especifica el algoritmo de cifrado utilizado para la conexión IKE. Esta configuración es válida únicamente si la opción "Tipo de VPN" se establece en "IPsec".
Algoritmo de integridad IKE	En la configuración se especifica el algoritmo de integridad utilizado para la conexión IKE. Esta configuración solo es válida si la opción "Tipo de VPN" se establece en "IPsec" y la "Versión IKE", en "IKEv2".
Grupo IPsec DH	Esta configuración especifica el grupo DH que un dispositivo utiliza para generar el material de clave. Los valores posibles son 0, 1, 2, 5, y de 14 a 26. El valor predeterminado es 0. Esta configuración es válida únicamente si la opción "Tipo de VPN" se establece en "IPsec".
Parámetro IPsec	En la configuración se especifica el parámetro IPsec utilizado para la conexión VPN. Esta configuración es válida únicamente si la opción "Tipo de VPN" se establece en "IPsec".

Android: configuración del perfil de VPN	Descripción
Confidencialidad directa total	En la configuración se especifica si la puerta de enlace VPN debe ser compatible con PFS. Esta configuración es válida únicamente si la opción "Tipo de VPN" se establece en "IPsec".
Activar MOBIKE	En la configuración se especifica si la puerta de enlace VPN debe ser compatible con MOBIKE. Esta configuración es válida únicamente si la opción "Tipo de VPN" se establece en "IPsec".
Duración de IPsec	En la configuración se especifica la duración, en segundos, de la conexión IPsec. Si establece un valor no admitido o un valor nulo, se usará el valor predeterminado del dispositivo. Esta configuración es válida únicamente si la opción "Tipo de VPN" se establece en "IPsec".
Algoritmo de cifrado IPsec	En la configuración se especifica el algoritmo de cifrado IPsec utilizado para la conexión VPN. Esta configuración es válida únicamente si la opción "Tipo de VPN" se establece en "IPsec".
Algoritmo de integridad IPsec	En la configuración se especifica el algoritmo de integridad IPsec utilizado para la conexión VPN. Esta configuración solo es válida si la opción "Tipo de VPN" se establece en "IPsec" y la "Versión IKE", en "IKEv2".
Tipo de autenticación	Esta configuración especifica el tipo de autenticación para la puerta de enlace VPN. Valores posibles: • Ninguno • Autenticación basada en certificados • Autenticación basada en CAC El valor predeterminado es "Ninguno". Esta configuración es válida únicamente si la opción "Tipo de VPN" se establece en "SSL".
Algoritmo SSL	En la configuración se especifica el algoritmo de cifrado necesario para la conexión VPN SSL. Esta configuración es válida únicamente si la opción "Tipo de VPN" se establece en "SSL".

Android: configuración del perfil de VPN	Descripción
Agregar información de UID/PID	En la configuración se especifica si se agregará información de UID y PID a los paquetes que se envían a la aplicación de cliente VPN. La configuración se debe seleccionar para la aplicación VPN de Cisco AnyConnect.
Cadenas compatibles	En la configuración se especifica cómo se admite la cadena VPN. Valores posibles: • Cadenas compatibles • Túnel exterior • Túnel interior El valor predeterminado es "Cadenas compatibles".
Tipo de entrada de cadena de proveedor	Esta configuración especifica los pares clave-valor o cadena JSON para la VPN. La información de configuración es específica de la aplicación VPN del proveedor. Valores posibles: • Pares clave-valor de proveedor • Valor de JSON de proveedor El valor predeterminado es "Pares clave-valor de proveedor".
Pares clave-valor de proveedor	En la configuración se especifican las claves y los valores asociados de VPN. La información de configuración es específica de la aplicación VPN del proveedor. Esta configuración es válida únicamente si la configuración "Tipo de entrada de cadena de proveedor" se establece en "Pares clave-valor de proveedor".
Valor de JSON de proveedor	Esta configuración especifica la información de configuración específica de la aplicación VPN del proveedor en formato .json. Esta configuración es válida únicamente si la configuración "Tipo de entrada de cadena de proveedor" se establece en "Valor de JSON de proveedor".
ID de paquete de cliente VPN	En la configuración se especifica el ID de paquete de la aplicación VPN.
Reintentar automáticamente la conexión tras un error	En la configuración se especifica si la conexión VPN se debería reiniciar automáticamente después de que se haya perdido la conexión.
Activar modo FIPS	En la configuración se especifica si el modo FIPS está activado. La activación del modo FIPS garantiza que solo se utilicen algoritmos de cifrado validados por FIPS para la conexión VPN.

Android: configuración del perfil de VPN	Descripción
Conectividad de la empresa para dispositivos Android con un espacio de trabajo	Esta configuración especifica si los dispositivos Samsung Knox Workspace utilizan una conexión VPN para todas las aplicaciones del espacio de trabajo o solo para las aplicaciones especificadas. • "VPN de todo el contenedor" utiliza una conexión VPN para todas las aplicaciones del espacio de trabajo en el dispositivo. • "VPN por aplicación" utiliza una conexión VPN solo para aplicaciones específicas.
Aplicaciones que pueden utilizar la conexión VPN	Esta configuración especifica las aplicaciones del espacio de trabajo que pueden utilizar una conexión VPN. Puede seleccionar aplicaciones en una lista de aplicaciones disponibles o especificar el ID de paquete de aplicación. Esta configuración es válida únicamente si la configuración "Conectividad de la empresa para dispositivos Android con un espacio de trabajo" se establece en "VPN por aplicación".
Perfil proxy asociado	Esta configuración especifica el perfil de proxy asociado que un dispositivo debe utilizar para conectarse al servidor proxy cuando el dispositivo está conectado a la red VPN.

Windows 10: Configuración de perfil VPN

Windows: Configuración de perfil VPN	Descripción
Tipo de conexión	En la configuración se especifica el tipo de conexión que un dispositivo Windows 10 debe utilizar para una VPN. Valores posibles: • Microsoft • Junos Pulse • SonicWALL Mobile Connect • F5 • Check Point Mobile • Definición de conexión manual El valor predeterminado es "Microsoft".
Servidor	En la configuración se especifica el nombre DNS o la dirección IP pública o enrutable para la puerta de enlace VPN. La configuración puede señalar a la IP externa de una VPN o a una IP virtual de una granja de servidores. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "Microsoft".

Windows: Configuración de perfil VPN	Descripción
Lista de URL de servidores	En la configuración se especifica una lista separada por comas de servidores con formato de URL, nombre de host o IP. Esta configuración es válida únicamente si la opción "Tipo de conexión" no se establece en "Microsoft".
Tipo de política de enrutamiento	En la configuración se especifica el tipo de política de enrutamiento. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "Microsoft". Valores posibles: • Dividir túnel • Forzar túnel El valor predeterminado es "Forzar túnel".
Tipo de protocolo nativo	En la configuración se especifica el tipo de política de enrutamiento que utiliza la VPN. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "Microsoft". Valores posibles: • L2TP • PPTP • IKEv2 • Automático El valor predeterminado es "Automático".
Autenticación	En la configuración se especifica el método de autenticación utilizado para la VPN nativa. La configuración "Tipo de protocolo nativo" determina qué tipos de autenticación son compatibles y el valor predeterminado de esta configuración: • Si selecciona L2TP o PPTP, los valores posibles son MS-CHAPv2 y EAP. El valor predeterminado es MS-CHAPv2. • Si selecciona IKEv2, los valores posibles son Método de usuario y Método de máquina. El valor predeterminado es Método de usuario. • Si selecciona Automático, el único valor posible es EAP. Valores posibles: • EAP • MS-CHAPv2 • Método de usuario • Método de máquina

Windows: Configuración de perfil VPN	Descripción
Configuración de EAP	Este ajuste especifica el valor XML de la configuración de EAP. Para obtener información acerca de cómo generar la configuración de EAP del valor XML, visite https://docs.microsoft.com/en-us/windows/client-management/mdm/eap-configuration Esta configuración es válida únicamente si la opción "Autenticación" se establece en "EAP".
Método de usuario	En la configuración se especifica el tipo de autenticación del método de usuario que se utiliza. Esta configuración es válida únicamente si la opción "Autenticación" se establece en "Método de usuario". Valores posibles: • EAP
Método de máquina	En la configuración se especifica el tipo de autenticación del método de máquina que se utiliza. Esta configuración es válida únicamente si la opción "Autenticación" se establece en "Método de máquina". Valor posible: • Certificado
Configuración personalizada	En la configuración se especifica el Blob XML codificado en HTML para una configuración específica del complemento SSL-VPN, incluida la información de autenticación enviada al dispositivo para que esté disponible para los complementos SSL-VPN. Esta configuración es válida únicamente si la opción "Tipo de conexión" no se establece en "Microsoft".
Nombre de la familia del paquete del complemento	En la configuración se especifica el nombre de la familia del paquete de la SSL VPN personalizada. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "Definición de conexión manual".
Clave compartida previamente de L2TP	Esta configuración especifica la clave compartida previamente que se debe utilizar para una conexión L2TP.
Lista de activadores de la aplicación	En la configuración se especifica una lista de aplicaciones que inician la conexión VPN.

Windows: Configuración de perfil VPN	Descripción
Lista de activadores de la aplicación > ID de la aplicación	En la configuración se especifica una aplicación para la VPN por aplicación. Valores posibles: • Nombre de la familia del paquete. Para encontrar el nombre de la familia del paquete, instale la aplicación y ejecute el comando de Windows PowerShell, `Get-AppxPackage`. Para obtener más información, visite http://technet.microsoft.com/en-us/library/hh856044.aspx • Ubicación de la instalación de la aplicación. Por ejemplo, C:\Windows\System\Notepad.exe.
Lista de rutas	En la configuración se especifica una lista de rutas que puede utilizar la VPN. Si la VPN utiliza la tunelización dividida, se requerirá una lista de rutas.
Dirección de subred	En la configuración se especifica la dirección IP del prefijo de destino con el formato de dirección IPv4 o IPv6.
Prefijo de subred	En la configuración se especifica el prefijo de subred del prefijo de destino.
Exclusión	Esta configuración especifica si la ruta que se ha agregado debe señalar a la interfaz VPN como la puerta de enlace o a una interfaz física. Si activa la casilla de verificación, el tráfico se dirige a través de la interfaz física. Si deja la casilla desactivada, el tráfico se dirige a través de la VPN.
Lista de nombres de dominio	En la configuración se especifican las reglas de la tabla NRPT (Name Resolution Policy Table, tabla de políticas de resolución de nombres) para la VPN.
Nombre de dominio	En la configuración se especifica el FQDN o sufijo del dominio.
Servidores DNS	En la configuración se especifica la lista de direcciones IP de los servidores DNS, separadas por comas.
Servidor proxy de la web	En la configuración se especifica la dirección IP del servidor proxy de la web.
Activar VPN	Esta configuración especifica si desea que esta regla de nombre de dominio active la VPN.
Persistente	Esta configuración especifica si desea que la regla de nombre de dominio se aplique cuando la VPN no esté conectada.
Lista de filtros de tráfico	En la configuración se especifican las reglas que permiten el tráfico a través de la VPN.

Windows: Configuración de perfil VPN	Descripción
Lista de filtros de tráfico > ID de la aplicación	En la configuración se especifica una aplicación para un filtro de tráfico basado en la aplicación. Valores posibles: • Nombre de la familia del paquete. Para encontrar el nombre de la familia del paquete, instale la aplicación y ejecute el comando de Windows PowerShell, `Get-AppxPackage`. Para obtener más información, visite http://technet.microsoft.com/en-us/library/hh856044.aspx • Ubicación de la instalación de la aplicación. Por ejemplo, `C:\Windows\System\Notepad.exe`. • Escriba "SYSTEM" para que los controladores de kernel puedan enviar el tráfico a través de VPN (por ejemplo, PING o SMB).
Protocolo	En la configuración se especifica el protocolo que utiliza la VPN. Valores posibles: • Todas • TCP • UDP El valor predeterminado es "Todo".
Intervalos de puertos locales	En la configuración se especifica la lista de intervalos de puertos locales permitidos, separados por comas. Por ejemplo, 100-120, 200, 300-320.
Intervalos de puertos remotos	En la configuración se especifica la lista de intervalos de puertos remotos permitidos, separados por comas. Por ejemplo, 100-120, 200, 300-320.
Intervalos de direcciones locales	En la configuración se especifica la lista de intervalos de direcciones IP locales permitidos, separados por comas.
Intervalos de direcciones remotas	En la configuración se especifica la lista de intervalos de direcciones IP remotas permitidos, separados por comas.
Tipo de política de enrutamiento	En la configuración se especifica la política de enrutamiento que utiliza el filtro de tráfico. Si se establece en "Forzar túnel", todo el tráfico pasa a través de la VPN. Si se establece en "Dividir túnel", el tráfico puede pasar a través de la VPN o de internet. Valores posibles: • Dividir túnel • Forzar túnel La configuración predeterminada es "Forzar túnel".
Recordar credenciales	En la configuración se especifica si las credenciales se almacenan en caché siempre que sea posible.

Windows: Configuración de perfil VPN	Descripción
Siempre activado	En la configuración se especifica si los dispositivos se conectarán automáticamente a la VPN al iniciar sesión y si se mantendrán conectados hasta que el usuario desconecte manualmente la VPN.
Bloqueo	Este ajuste especifica si la conexión VPN se debe usar cuando el dispositivo se conecta a una red. Cuando esta opción está activada, se aplica lo siguiente: • El dispositivo permanece conectado a la VPN. No puede desconectarse. • El dispositivo debe estar conectado a esta red VPN para utilizar cualquier conexión de red. • El dispositivo no puede conectarse a, o modificar, otros perfiles VPN.
Sufijo DNS	En la configuración se especifican uno o varios sufijos DNS separados por comas. El primer sufijo DNS de la lista también se empleará como la conexión principal para la VPN. La lista se agrega a la lista de búsqueda de sufijos.
Detección de redes de confianza	En la configuración se especifica una cadena separada por comas para identificar las redes de confianza. La VPN no se conecta automáticamente cuando los usuarios están en la red inalámbrica de la empresa.
Propiedades de seguridad IP	
Constantes de transformación de autenticación	Valores posibles: • MD596 • SHA196 • SHA256128 • GCMAES128 • GCMAE192 • GCMAES256 La configuración predeterminada es "MD596".
Constantes de transformación de cifrado	Valores posibles: • DES • DES3 • AES128 • AES192 • AES256 • GCMAES128 • GCMAES192 • GCMAES256 La configuración predeterminada es "DES".

Windows: Configuración de perfil VPN	Descripción
Método de cifrado	Valores posibles: • DES • DES3 • AES128 • AES192 • AES256 La configuración predeterminada es "DES".
Método de comprobación de integridad	Valores posibles: • MD5 • SHA196 • SHA256 • SHA384 La configuración predeterminada es "MD5".
Grupo Diffie-Hellman	Valores posibles: • Group1 • Group2 • Group14 • ECP256 • ECP384 • Group24 La configuración predeterminada es "Group1".
Grupo PFS	Valores posibles: • PFS1 • PFS2 • PFS2048 • ECP256 • ECP384 • PFSMM • PFS24 El valor predeterminado es "PFS1".
Tipo de proxy	Esta configuración especifica el tipo de configuración de proxy para la VPN. Valores posibles: • Ninguno • Configuración de PAC • Configuración manual El valor predeterminado es "Ninguno".

Windows: Configuración de perfil VPN	Descripción
URL de PAC	En la configuración se especifica la URL del servidor web que aloja el archivo de PAC incluido el nombre del archivo. Por ejemplo, http://www.example.com/PACfile.pac. Esta configuración es válida únicamente si la opción "Tipo de proxy" se establece en "Configuración de PAC".
Dirección	En la configuración se especifican las direcciones FQDN o IP del servidor proxy. Esta configuración es válida únicamente si la opción "Tipo de proxy" se establece en "Configuración manual".
Perfil SCEP asociado	En la configuración se especifica el perfil SCEP asociado que un dispositivo debe utilizar para obtener un certificado de cliente con el objetivo de autenticarlo con la VPN .

Activación de una VPN por aplicación

Puede configurar una VPN por aplicación en los dispositivos con iOS, iPadOS, Samsung Knox y Windows 10 para especificar qué aplicaciones de los dispositivos deben utilizar una VPN para sus datos en tránsito. VPN por aplicación contribuye a disminuir la carga de la VPN de la empresa al permitir que solo parte del tráfico de trabajo utilice la VPN (por ejemplo, al acceder a servidores de aplicaciones o páginas web que están detrás del firewall). En entornos locales, esta característica también es compatible con la privacidad del usuario y aumenta la velocidad de conexión de las aplicaciones personales al no enviar el tráfico personal a través de la VPN.

Para los dispositivos con iOS y iPadOS, las aplicaciones se asocian a un perfil de VPN cuando asigna la aplicación o grupo de aplicaciones a un usuario, grupo de usuarios o grupo de dispositivos.

Para los dispositivos Samsung Knox con activaciones de Android Enterprise y Samsung Knox Workspace, las aplicaciones se agregan a la configuración "Aplicaciones que pueden utilizar la conexión VPN" en el perfil de VPN.

Para los dispositivos con Windows 10, las aplicaciones se agregan a la configuración "Lista de activadores de la aplicación" en el perfil de VPN.

¿Cómo BlackBerry UEM elige qué ajustes de VPN por aplicación se asignan a dispositivos con iOS ?

Solo se puede asignar un perfil de VPN a una aplicación o grupo de aplicaciones. BlackBerry UEM utiliza las siguientes reglas para determinar qué ajustes de VPN por aplicación asignar a una aplicación en los dispositivos iOS y iPadOS:

- Los ajustes de VPN por aplicación que se asocian directamente a una aplicación tienen prioridad sobre los ajustes de VPN por aplicación asociados indirectamente a un grupo de aplicaciones.
- Los ajustes de VPN por aplicación que se asocian directamente a un usuario tienen prioridad sobre los ajustes de VPN por aplicación asociados indirectamente a un grupo de usuarios.
- Los ajustes de VPN por aplicación que se asignan a una aplicación obligatoria tienen prioridad sobre los ajustes de VPN por aplicación asignados a una instancia opcional de la misma aplicación.
- Los ajustes de VPN por aplicación que se asocian al nombre del grupo de usuarios que aparece anteriormente en la lista alfabética tienen prioridad si se cumplen las siguientes condiciones:
  - Se asigna una aplicación a varios grupos de usuarios
  - La misma aplicación aparece en los grupos de usuarios

- Se asigna la aplicación del mismo modo, ya sea como una sola aplicación o como un grupo de aplicaciones
- La aplicación tiene la misma disposición en todas las asignaciones, ya sea obligatoria u opcional

  Por ejemplo, puede asignar Cisco WebEx Meetings como una aplicación opcional a los grupos de usuarios de desarrollo y marketing. Cuando un usuario se encuentra en ambos grupos, los ajustes de VPN por aplicación para el grupo de desarrollo se aplican a la aplicación WebEx Meetings para dicho usuario.

Si el perfil de VPN por aplicación se asigna a un grupo de dispositivos, tiene prioridad sobre el perfil de VPN por aplicación que se asigna a la cuenta de usuario para los dispositivos que pertenecen al grupo de dispositivos.

Configuración de los perfiles de proxy para dispositivos

Puede especificar la forma de uso de un servidor proxy de los dispositivos para acceder a servicios web en Internet o en una red de trabajo. Para los dispositivos con iOS, iPadOS, macOS y Android se crea un perfil de proxy. Para los dispositivos con Windows 10, puede agregar los ajustes de proxy en el perfil de Wi-Fi o de VPN.

A menos que se indique lo contrario, los perfiles de proxy son compatibles con los servidores proxy con autenticación básica o sin ella.

Dispositivo	Configuración de proxy
iOS y iPadOS	Cree un perfil de proxy y asócielo con los perfiles que utiliza la empresa, que puede incluir cualquiera de los siguientes: • Wi-Fi • VPN También se puede asignar un perfil de proxy a cuentas de usuarios, a grupos de usuarios y a grupos de dispositivos. **Nota:** Un perfil de proxy que se asigna a cuentas de usuario, a grupos de usuarios o a grupos de dispositivos es un proxy global para los dispositivos supervisados únicamente y tiene prioridad sobre un perfil de proxy que esté asociado a un perfil de Wi-Fi o de VPN. Los dispositivos supervisados utilizarán la configuración de proxy global para todas las conexiones HTTP.
macOS	Cree un perfil de proxy y asócielo a un perfil Wi-Fio de VPN. macOS aplica perfiles a las cuentas de usuario o los dispositivos. Los perfiles de proxy se aplican a los dispositivos.
Android	Para dispositivos con Android Enterprise, cree un perfil de proxy y asócielo a un perfil de Wi-Fi. Los dispositivos Android 8.0 y versiones posteriores con Controles de MDM o Privacidad del usuario no son compatibles con perfiles de Wi-Fi con configuración de proxy.

Dispositivo	Configuración de proxy
Samsung Knox	Cree un perfil de proxy y asócielo a los perfiles que utiliza la empresa. Se aplican las siguientes condiciones: • Para los perfiles Wi-Fi, solo los perfiles de proxy con la configuración manual son compatibles con los dispositivos con Knox. Los perfiles de proxy que se asocien a los perfiles de Wi-Fi son compatibles con los servidores proxy con autenticación básica, NTLM o sin autenticación. • Para los perfiles VPN y de conectividad de la empresa, los perfiles de proxy con la configuración manual son compatibles con los dispositivos con Samsung Knox con activaciones de Android Enterprise y los dispositivos con Samsung Knox Workspace que utilicen Knox 2.5 o posterior. Los perfiles de proxy con la configuración de PAC son compatibles con los dispositivos conSamsung Knox con activaciones de Android Enterprise y los dispositivos con Knox Workspace que utilizan una versión de Knox posterior a 2.5. **Nota:** Para utilizar perfil de proxy con un perfil de conectividad de la empresa, BlackBerry Secure Connect Plus debe estar activado. También se puede asignar un perfil de proxy a cuentas de usuarios, a grupos de usuarios y a grupos de dispositivos. Se aplican las siguientes condiciones: • En los dispositivos con Knox Workspace y Samsung Knox con activaciones de Android Enterprise, el perfil configura las opciones de proxy del navegador en el espacio de trabajo. • En los dispositivos con Samsung Knox MDM, el perfil configura las opciones de proxy del navegador en el dispositivo. **Nota:** La Configuración de PAC no es compatible con los dispositivos Knox Workspace que utilizan Knox 2.5 y versiones anteriores y con los dispositivos con Knox MDM.
Windows 10	Cree un perfil de Wi-Fi o de VPN y especifique la información del servidor proxy en los ajustes del perfil. Se aplican las siguientes condiciones: • El proxy de Wi-Fi solo admite la configuración manual y únicamente es compatible con los dispositivos con Windows 10 Mobile. • Proxy VPN admite PAC o configuración manual.

Creación de un perfil de proxy

Si la empresa utiliza un archivo PAC para definir las reglas de proxy, puede seleccionar la configuración de PAC para utilizar el servidor proxy desde el archivo PAC que especifique. De lo contrario, puede seleccionar la configuración manual y especificar la configuración del servidor proxy directamente en el perfil.

1. En la barra de menú, haga clic en **Políticas y perfiles**.
2. Haga clic en **Redes y conexiones > Proxy**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil de proxy.
5. Haga clic en la pestaña de un tipo de dispositivo.
6. Lleve a cabo una de las tareas siguientes:

Tarea	Pasos
Especificar los ajustes de configuración de PAC	**a.** En la lista desplegable **Tipo**, compruebe que está seleccionada la opción **Configuración de PAC**. **b.** En el campo **URL de PAC**, escriba la URL para el servidor web que aloja el archivo de PAC e incluya el nombre del archivo (por ejemplo, http://www.example.com/PACfile.pac). El archivo PAC no debe alojarse en un servidor que aloje BlackBerry UEM ni ninguno de sus componentes. **c.** En la pestaña **BlackBerry**, lleve a cabo las acciones siguientes: **1.** Si la empresa requiere que los usuarios proporcionen un nombre de usuario y una contraseña para conectarse al servidor proxy y el perfil es para varios usuarios, en el campo **Nombre de usuario** escriba `%UserName%`. Si el servidor proxy solicita el nombre de dominio para la autenticación, utilice el formato *<dominio>\<nombre de usuario>*. **2.** En la lista desplegable **El usuario puede editar**, haga clic en los ajustes de proxy que los usuarios de dispositivos con BlackBerry 10 pueden cambiar. La configuración predeterminada es **Solo lectura**.
Especificar los ajustes de configuración manual	**a.** En la lista desplegable **Tipo**, haga clic en **Configuración manual**. **b.** En el campo **Host**, escriba la dirección FQDN o IP del servidor proxy. **c.** En el campo **Puerto**, escriba el número de puerto del servidor proxy. **d.** Si la empresa requiere que los usuarios proporcionen un nombre de usuario y una contraseña para conectarse al servidor proxy y el perfil es para varios usuarios, en el campo **Nombre de usuario** escriba `%UserName%`. Si el servidor proxy solicita el nombre de dominio para la autenticación, utilice el formato *<dominio>\<nombre de usuario>*. **e.** En la pestaña **BlackBerry**, lleve a cabo las acciones siguientes: **1.** En la lista desplegable **El usuario puede editar**, haga clic en los ajustes de proxy que los usuarios de dispositivos con BlackBerry 10 pueden cambiar. La configuración predeterminada es **Solo lectura**. **2.** Opcionalmente, puede especificar una lista de direcciones a las que los usuarios puedan acceder directamente desde los dispositivos con BlackBerry 10 sin utilizar el servidor proxy. En el campo **Lista de exclusión**, escriba las direcciones (FQDN o IP) y utilice un punto y coma (;) para separar los valores de la lista. Puede utilizar el carácter comodín (*) en un FQDN o IP (por ejemplo, *.ejemplo.com o 192.0.2.*).

7. Repita los pasos 4 y 5 para cada tipo de dispositivo en la empresa.
8. Haga clic en **Agregar**.

Después de terminar:

- Asocie el perfil de proxy con un perfil de Wi-Fi, de VPN o de conectividad de la empresa.
- Si fuera necesario, clasifique los perfiles. La clasificación que se especifique solo se aplicará si se asigna un perfil de proxy a los grupos de usuarios o de dispositivos.

Uso de BlackBerry Secure Connect Plus para establecer conexiones a los recursos del trabajo

BlackBerry Secure Connect Plus es un componente de BlackBerry UEM que proporciona un túnel IP seguro entre las aplicaciones y la red de la empresa:

- En los dispositivos con Android Enterprise, todas las aplicaciones de trabajo usan el túnel seguro.
- En los dispositivos con Samsung Knox Workspace y Samsung Knox con activaciones de Android Enterprise, puede permitir que todas las aplicaciones del espacio de trabajo utilicen el túnel o especificar aplicaciones mediante una VPN por aplicación.
- En los dispositivos con iOS y iPadOS, puede permitir que todas las aplicaciones utilicen el túnel o especificar aplicaciones mediante una VPN por aplicación.

Nota: Si BlackBerry Secure Connect Plus no está disponible en su región, debe desactivarlo manualmente para los dispositivos Android en el perfil de conectividad de la empresa.

Este túnel IP seguro proporciona a los usuarios acceso a los recursos de trabajo detrás del firewall de la empresa, lo que garantiza que los datos estén protegidos mediante protocolos estándar y cifrado integral.

BlackBerry Secure Connect Plus y un dispositivo compatible establecen un túnel IP seguro cuando se trata de la mejor opción disponible para realizar la conexión a la red de la empresa. Si se asigna un perfil Wi-Fi o un perfil VPN a un dispositivo y el dispositivo puede acceder a la red Wi-Fi o VPN del trabajo, el dispositivo utilizará estos métodos para conectarse a la red. Si estas opciones no están disponibles (por ejemplo, si el usuario no se encuentra dentro del alcance de la red Wi-Fi del trabajo), BlackBerry Secure Connect Plus y el dispositivo establecerán un túnel IP seguro.

En los dispositivos iOS y iPadOS, si configura una red VPN por aplicación para BlackBerry Secure Connect Plus, las aplicaciones configuradas siempre utilizarán una conexión de túnel segura a través de BlackBerry Secure Connect Plus, incluso si la aplicación puede conectarse a la red Wi-Fi de trabajo o VPN especificada en un perfil de VPN.

Los dispositivos compatibles se comunican con BlackBerry UEM para establecer un túnel seguro a través de BlackBerry Infrastructure. Se establece un túnel para cada dispositivo. El túnel es compatible con los protocolos IPv4 estándar (TCP y UDP) y el tráfico IP que se envía entre los dispositivos y BlackBerry UEM está cifrado de manera integral mediante AES256. Mientras el túnel esté abierto, las aplicaciones puede acceder a los recursos de la red. Cuando el túnel ya no sea necesario (por ejemplo, si el usuario se encuentra dentro del alcance de la red Wi-Fi del trabajo), se dará por finalizado.

Para obtener más información acerca de cómo BlackBerry Secure Connect Plus transfiere datos a y desde los dispositivos, consulte el contenido referente a Arquitectura local o el contenido referente a Arquitectura en la nube.

Pasos para activar BlackBerry Secure Connect Plus

Para activar BlackBerry Secure Connect Plus, siga los pasos siguientes:

Paso	Acción
1	Verifique que el dominio de BlackBerry UEM de la empresa cumple los requisitos para utilizar BlackBerry Secure Connect Plus.

Paso	Acción
2	Si tiene BlackBerry UEM Cloud, instale el BlackBerry Connectivity Node o actualice el BlackBerry Connectivity Node a la versión más reciente.
3	Active BlackBerry Secure Connect Plus en el perfil de conectividad de empresa predeterminado o en un perfil de conectividad de la empresa personalizado que haya creado.
4	De manera opcional, especifique la configuración DNS adecuada para la aplicación BlackBerry Connectivity.
5	Si tiene un entorno local que incluye dispositivos Android Enterprise y Samsung Knox Workspace activados con BlackBerry Dynamics, optimice las conexiones de túnel seguras.
6	Asigne el perfil de conectividad de empresa a cuentas de usuarios de https://docs.blackberry.com/es/endpoint-management/blackberry-uem/current/administration/users-groups/adr1374514829642/assign-app-to-user.html o a grupos de usuarios dehttps://docs.blackberry.com/es/endpoint-management/blackberry-uem/current/administration/users-groups/hse1372277059163/assign-app-to-user-group.html.

Requisitos del servidor y del dispositivo para BlackBerry Secure Connect Plus

Para utilizar BlackBerry Secure Connect Plus, el entorno de la empresa debe cumplir con los requisitos siguientes.

Para el dominio de BlackBerry UEM:

- El firewall de la empresa debe permitir conexiones salientes a través del puerto 3101 a *<región>*.turnb.bbsecure.com y *<región>*.bbsecure.com. Si configura BlackBerry UEM para que utilice un servidor proxy, verifique que dicho servidor permita conexiones a estos subdominios a través del puerto 3101. Para obtener más información acerca de los dominios y las direcciones IP que puede utilizar en la configuración de firewall, visite http://support.blackberry.com/community y lea el artículo 36470.
- En cada instancia de BlackBerry UEM, el componente de BlackBerry Secure Connect Plus debe estar ejecutándose.
- De forma predeterminada, los dispositivos Android Enterprise tienen restringido el uso de BlackBerry Secure Connect Plus para conectarse a Google Play y los servicios subyacentes (com.android.providers.media, com.android.vending, and com.google.android.apps.gcs). Google Play no cuenta con compatibilidad de proxy. Los dispositivos Android Enterprise utilizan una conexión directa a través de Internet a Google Play. Estas restricciones están configuradas en el perfil de conectividad de la empresa predeterminado y en cualquier perfil de conectividad de la empresa nuevo que cree. Se recomienda mantener estas restricciones. Si elimina estas restricciones, debe ponerse en contacto con el soporte de Google Play para conocer la configuración de cortafuegos necesaria para permitir las conexiones a Google Play mediante BlackBerry Secure Connect Plus.
- Si tiene BlackBerry UEM Cloud, debe instalar el BlackBerry Connectivity Node o actualizarlo a la última versión.

Nota: Si su entorno local incluye dispositivos con Knox Workspace o Android Enterprise con aplicaciones de BlackBerry Dynamics, consulte Optimización de las conexiones de túnel seguras para dispositivos Android que utilizan aplicaciones de BlackBerry Dynamics.

Nota: Si utiliza un perfil de correo para activar BlackBerry Secure Gateway para dispositivos iOS, se recomienda configurar una VPN por aplicación para BlackBerry Secure Connect Plus. Para obtener más información sobre

BlackBerry Secure Gateway, consulte Protección de los datos de correo electrónico con BlackBerry Secure Gateway.

En los dispositivos compatibles:

Dispositivo	Requisitos
iOS y iPadOS	• Los dispositivos deben activarse mediante BlackBerry UEM Client, disponible en App Store • Tipo de activación de Controles de MDM

Android Enterprise	• Cualquiera de los tipos de activación siguientes:
	  • Solo espacio de trabajo (Premium)
	  • Trabajo y personal: control total (Premium)
	  • Trabajo y personal: privacidad de usuario (Premium)

Samsung Knox Workspace	• Samsung Knox MDM 5.0 o posteriores
	• Samsung Knox 2.3 o posteriores
	• Cualquiera de los tipos de activación siguientes:
	  • Solo espacio de trabajo (Samsung Knox)
	  • Trabajo y personal: control total (Samsung Knox)
	  • Trabajo y personal: privacidad de usuario (Samsung Knox)

Instalación de componentes de BlackBerry Secure Connect Plus adicionales en un entorno local

Puede instalar una o varias instancias de BlackBerry Connectivity Node para agregar instancias adicionales de los componentes de conectividad del dispositivo al dominio de su empresa. Cada BlackBerry Connectivity Node contiene una instancia activa de BlackBerry Secure Connect Plus que puede procesar los datos de dispositivo y establecer conexiones seguras.

También puede crear grupos de servidores. Un grupo de servidores contiene una o más instancias de BlackBerry Connectivity Node. Al crear un grupo de servidores, debe especificar la ruta de datos regionales que desea que los componentes usen para conectarse a BlackBerry Infrastructure. Por ejemplo, puede crear un grupo de servidores para dirigir las conexiones de dispositivo para BlackBerry Secure Connect Plus y BlackBerry Secure Gateway para usar la ruta de Estados Unidos a BlackBerry Infrastructure. Puede asociar perfiles de correo y de conectividad de empresa con un grupo de servidores. Cualquier dispositivo que se asigne a estos perfiles usa la conexión regional del grupo de servidores a BlackBerry Infrastructure cuando utiliza cualquiera de los componentes de BlackBerry Connectivity Node.

Si un dominio incluye más de una instancia de BlackBerry UEM, el componente de BlackBerry Secure Connect Plus de cada instancia ejecuta y procesa datos. Los datos se cargan de forma equilibrada en todos los componentes de BlackBerry Secure Connect Plus del dominio.

El conmutador por error de alta disponibilidad está disponible en BlackBerry Secure Connect Plus. Si un dispositivo está utilizando un túnel seguro y el componente de BlackBerry Secure Connect Plus actual deja de estar disponible, BlackBerry Infrastructure asignará el dispositivo a un componente de BlackBerry Secure Connect Plus de otra instancia de BlackBerry UEM. El dispositivo reanuda la utilización del túnel seguro con una interrupción mínima.

Para obtener más información sobre la planificación y la instalación de un BlackBerry Connectivity Node, consulte el contenido sobre Planificación de contenido y el contenido de instalación y de actualización.

Instalación o actualización del componente de BlackBerry Secure Connect Plus en un entorno en la nube

Al instalar BlackBerry Connectivity Node, el proceso de configuración también instala el componente BlackBerry Secure Connect Plus en el mismo ordenador. Si actualiza BlackBerry Connectivity Node a la última versión y BlackBerry Secure Connect Plus no está instalado, el proceso de actualización instala BlackBerry Secure Connect Plus. Si BlackBerry Secure Connect Plus se ha instalado previamente, el proceso actualiza BlackBerry Secure Connect Plus a la última versión.

Para obtener instrucciones sobre cómo instalar o actualizar BlackBerry Connectivity Node, consulte "Instalación y actualización de BlackBerry Connectivity Node" en el contenido de Configuración de BlackBerry UEM Cloud. Debe activar BlackBerry Connectivity Node antes de activar BlackBerry Secure Connect Plus.

Tiene la opción de enrutar los datos que se transmiten entre BlackBerry Secure Connect Plus y BlackBerry Infrastructure a través de un servidor proxy TCP (transparente o SOCKS v5). Puede configurar el proxy mediante la consola de administración de BlackBerry Connectivity Node (Configuración general > Proxy).

Nota: Si especifica información de proxy no válida, BlackBerry Secure Connect Plus deja de ejecutarse y no se puede reiniciar. Si se produce este problema, corrija la información del proxy y reinicie el servicio de BlackBerry UEM - BlackBerry Secure Connect Plus en los servicios de Windows.

Puede instalar un segundo BlackBerry Connectivity Node para la redundancia. Ambas instancias de BlackBerry Secure Connect Plus ejecutan y procesan datos. La carga de datos se equilibra en las dos instancias. Si un dispositivo está utilizando un túnel seguro y la instancia de BlackBerry Secure Connect Plus actual deja de estar disponible, BlackBerry Infrastructure asignará el dispositivo a la otra instancia. El dispositivo reanuda la utilización del túnel seguro con una interrupción mínima.

Activar BlackBerry Secure Connect Plus

Para permitir que los dispositivos utilicen BlackBerry Secure Connect Plus, deberá activar BlackBerry Secure Connect Plus en un perfil de conectividad de la empresa y asignar el perfil a los usuarios y grupos.

Al aplicar el perfil de conectividad de empresa al dispositivo después de la activación, BlackBerry UEM instala la aplicación BlackBerry Connectivity en el dispositivo (para dispositivos Android Enterprise, la aplicación se instala automáticamente desde Google Play; para dispositivos con iOS y iPadOS, la aplicación se instala automáticamente desde App Store).

BlackBerry lanza nuevas versiones de la aplicación para permitir nuevas mejoras y funciones. Para obtener instrucciones sobre la actualización de la aplicación y recibir información acerca de los últimos problemas conocidos y resueltos, consulte las notas de la versión de la aplicación BlackBerry Connectivity.

1. En la consola de gestión, en la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Redes y conexiones > Conectividad de empresa**.
3. Haga clic en +.
4. Si ha creado y configurado uno o más grupos de servidores para dirigir el tráfico de BlackBerry Secure Connect Plus a un ruta regional específica a BlackBerry Infrastructure, en la lista desplegable **Grupo de servidores de BlackBerry Secure Connect Plus**, haga clic en el grupo de servidores correspondiente.

5. Configure los valores correspondientes de la configuración de perfil de cada tipo de dispositivo. Para obtener más información acerca de la configuración de cada perfil, consulte Configuración del perfil de conectividad de empresa.
6. Haga clic en **Agregar**.
7. Asigne el perfil a las cuentas de grupos o usuarios.
8. Si ha configurado VPN por aplicación para dispositivos iOS y iPadOS, al asignar una aplicación o grupo de aplicaciones, asócielo con el perfil de conectividad de la empresa adecuado.

Después de terminar:

- En los dispositivos Android Enterprise y Samsung Knox Workspace, la aplicación de BlackBerry Connectivity solicitará a los usuarios que la ejecuten como una VPN y que le permitan el acceso a las claves privadas del dispositivo. Instruya a los usuarios para aceptar las solicitudes. Los usuarios de dispositivos con iOS, iPadOS, Android Enterprise y Knox Workspace pueden abrir la aplicación para ver el estado de la conexión. No se requiere ninguna otra acción de los usuarios.
- Si crea más de un perfil de conectividad de la empresa, clasifique los perfiles.
- Si está solucionando un problema de conexión con un dispositivo con iOS, iPadOS, Android Enterprise o Knox Workspace, la aplicación permite al usuario enviar los registros del dispositivo a una dirección de correo del administrador (el usuario introduce una dirección de correo electrónico que usted debe proporcionar). Tenga en cuenta que los registros no son visibles con Winzip. Se recomienda utilizar otra utilidad como 7-Zip.

Configuración del perfil de conectividad de empresa

Los perfiles de conectividad de empresa son compatibles con los siguientes tipos de dispositivos:

- iOS
- iPadOS
- Android

Común: configuración del perfil de conectividad de empresa

Común: configuración del perfil de conformidad	Descripción
Grupo de servidores de BlackBerry Secure Connect Plus	Esta configuración especifica el grupo de servidores que utiliza BlackBerry Secure Connect Plus para dirigir el tráfico a una ruta regional específica. Esta configuración es válida únicamente si ha instalado una o más instancias de BlackBerry Connectivity Node y configurado los grupos de servidores.

iOS: configuración del perfil de conectividad de empresa

Esta configuración para iOS se aplica también a dispositivos con iPadOS.

Configuración	Descripción
Activar BlackBerry Secure Connect Plus	Esta configuración especifica si las aplicaciones de trabajo utilizan BlackBerry Secure Connect Plus para enviar los datos de trabajo entre los dispositivos y la red.

Configuración	Descripción
Activar VPN a petición	Seleccione esta comunicación para permitir que solo aplicaciones específicas utilicen BlackBerry Secure Connect Plus. **Nota:** Si selecciona esta opción, los usuarios deben activar manualmente la conexión VPN en su dispositivo para utilizar BlackBerry Secure Connect Plus. Mientras la conexión VPN está activada, el dispositivo utiliza BlackBerry Secure Connect Plus para conectarse a la red del trabajo. El usuario debe activar la conexión VPN para utilizar otra conexión, como la red Wi-Fi del trabajo. Indique a los usuarios cuándo es el momento adecuado para activar y desactivar la conexión VPN (por ejemplo, puede indicarles que activen la conexión VPN cuando no están dentro del alcance de la red Wi-Fi del trabajo).
Reglas de VPN a petición para iOS 9 y posteriores	Esta configuración especifica los requisitos de conexión para VPN a petición utilizando BlackBerry Secure Connect Plus. Debe utilizar una o más claves del ejemplo de formato de carga. Esta configuración es válida únicamente si se ha seleccionado la opción "Activar VPN a petición".
Activar VPN por aplicación	Esta configuración especifica si una aplicación de trabajo puede iniciar una conexión VPN utilizando BlackBerry Secure Connect Plus cuando accede a los recursos de trabajo. Seleccione esta configuración para especificar reglas para las conexiones de BlackBerry Secure Connect Plus.
Dominios de Safari	Haga clic en + para especificar los dominios que tienen permitido iniciar una conexión VPN en Safari.
Permitir la conexión automática de aplicaciones	Especifique si las aplicaciones pueden iniciar automáticamente la conexión VPN.
Perfil de proxy	Esta configuración especifica el perfil de proxy asociado si desea enrutar el tráfico de túnel seguro de los dispositivos a la red del trabajo a través de un servidor proxy. El perfil de proxy debe utilizar una configuración manual con una dirección IP. No se admite la configuración de PAC. Para obtener más información, consulte Configuración de los perfiles de proxy para dispositivos.

Android: Configuración del perfil de conectividad de empresa

Configuración	Descripción
Activar BlackBerry Secure Connect Plus	Esta configuración especifica si las aplicaciones de trabajo utilizan BlackBerry Secure Connect Plus para enviar los datos de trabajo entre los dispositivos y la red.

Configuración	Descripción
Conectividad de la empresa para dispositivos Android con un espacio de trabajo	Esta configuración especifica si los dispositivos Android Enterprise y Samsung Knox Workspace utilizan BlackBerry Secure Connect Plus para todas las aplicaciones del espacio de trabajo o solo para las aplicaciones especificadas. • "VPN de todo el contenedor" utiliza una conexión VPN para todas las aplicaciones del espacio de trabajo en el dispositivo. • "VPN por aplicación" utiliza una conexión VPN solo para aplicaciones específicas.
Aplicaciones con uso restringido de BlackBerry Secure Connect Plus	Esta configuración especifica las aplicaciones del espacio de trabajo en dispositivos Android Enterprise que no pueden utilizar BlackBerry Secure Connect Plus. Haga clic en + y escriba el ID de paquete de aplicación. Repita según sea necesario para restringir aplicaciones adicionales. De forma predeterminada, Google Play y los servicios subyacentes (com.android.providers.media, com.android.vending, com.google.android.gms y com.google.android.apps.gcs) están restringidos porque Google Play no cuenta con soporte de proxy. Se recomienda mantener estas restricciones. Si elimina cualquiera de estas restricciones, debe ponerse en contacto con el soporte de Google Play para conocer la configuración de cortafuegos necesaria para permitir las conexiones a Google Play mediante BlackBerry Secure Connect Plus. De forma predeterminada, los paquetes se agregan al nuevo perfil de conectividad de la empresa; sin embargo, debe agregarlos a cualquier perfil existente. Si se aplica la política de TI "Forzar que las aplicaciones de trabajo solo utilicen VPN" al dispositivo, esta configuración se ignora y no se impide que las aplicaciones de trabajo, incluidas las aplicaciones BlackBerry UEM Client y Google Play utilicen BlackBerry Secure Connect Plus. En ese caso, deberá abrir los puertos del firewall para permitir que BlackBerry UEM Client se comunique con BlackBerry Infrastructure a través de BlackBerry UEM. Para obtener más información acerca de cómo abrir los puertos del firewall cuando las aplicaciones de trabajo utilizan BlackBerry Secure Connect Plus, visite support.blackberry.com/community para leer el artículo 48330. Si su empresa utiliza aplicaciones de BlackBerry Dynamics, se recomienda que restrinja que las aplicaciones usen BlackBerry Secure Connect Plus. De lo contrario, debe abrir puertos adicionales en el firewall de su empresa para permitir que las aplicaciones envíen datos a BlackBerry Dynamics NOC, y la actividad de red de las aplicaciones puede retrasarse debido a que los datos se enrutan a BlackBerry Infrastructure y BlackBerry Dynamics NOC. Esta configuración es válida únicamente si la configuración "Conectividad de la empresa para dispositivos Android con un espacio de trabajo" se establece en "VPN de todo el contenedor".

Configuración	Descripción
Aplicaciones con permiso para usar Enterprise Connectivity	Esta configuración especifica las aplicaciones del espacio de trabajo de los dispositivos Android Enterprise y Samsung Knox Workspace que pueden utilizar BlackBerry Secure Connect Plus. Puede seleccionar aplicaciones en una lista de aplicaciones disponibles o especificar el ID de paquete de aplicación. Esta configuración es válida únicamente si la configuración "Conectividad de la empresa para dispositivos Android con un espacio de trabajo" se establece en "VPN por aplicación".
Perfil de proxy	Si desea enrutar el tráfico de túnel seguro desde los dispositivos Samsung Knox con activaciones de Android Enterprise y los dispositivos Samsung Knox Workspace 2.5 o posteriores a la red del trabajo a través de un servidor proxy, seleccione el perfil de proxy adecuado. Esta configuración no se aplica a los dispositivos Android Enterprise que no sean Samsung Knox ni a los dispositivos Samsung Knox Workspace de la versión 2.4 o anterior.

Especificar la configuración del DNS adecuada para la aplicación de BlackBerry Connectivity

Puede especificar los servidores DNS que desea que la aplicación BlackBerry Connectivity utilice en las conexiones de túnel seguro. También puede especificar los sufijos de búsqueda de DNS. Si no se especifica la configuración DNS, la aplicación obtendrá las direcciones DNS del equipo que aloja el componente de BlackBerry Secure Connect Plus y el sufijo de búsqueda predeterminado será el dominio DNS de ese equipo.

Si crea o configura uno o más grupos de servidores para dirigir las conexiones de BlackBerry Secure Connect Plus a una ruta regional a BlackBerry Infrastructure, puede especificar la configuración de DNS determinada para cada grupo de servidores. Si lo hace, la configuración DNS de un grupo de servidores tiene prioridad sobre la configuración de DNS global que se especifique mediante los siguientes pasos. Para obtener más información acerca de la creación y configuración de grupos de servidores, consulte el contenido de Instalación y actualización local o el contenido de Configuración de UEM Cloud.

1. Lleve a cabo una de las siguientes acciones:
   - En un entorno local, en la consola de gestión de UEM, haga clic en **Configuración > Infraestructura > BlackBerry Secure Connect Plus** en la barra de menús.
   - En un entorno en la nube, en la consola de BlackBerry Connectivity Node (http:/localhost:8088), haga clic en el panel izquierdo en **Configuración general > BlackBerry Secure Connect Plus**.
2. Active la casilla de verificación **Configurar manualmente los servidores DNS** y haga clic en +.
3. Escriba la dirección del servidor DNS con notación decimal con puntos (por ejemplo, 192.0.2.0). Haga clic en **Agregar**.
4. Si fuera necesario, repita los pasos 2 y 3 para agregar más servidores DNS. En la tabla **Servidores DNS**, haga clic en las flechas de la columna **Clasificación** para establecer la prioridad de los servidores DNS.
5. Si desea especificar los sufijos de búsqueda de DNS, realice los pasos siguientes:
   a) Active la casilla de verificación **Gestionar los sufijos de búsqueda de DNS manualmente** y haga clic en +.
   b) Escriba el sufijo de búsqueda de DNS (por ejemplo, domain.com). Haga clic en **Agregar**.

6. Si fuera necesario, repita el paso 5 para agregar más sufijos de búsqueda de DNS. En la tabla **Sufijos de búsqueda de DNS**, haga clic en las flechas de la columna **Clasificación** para establecer la prioridad de los servidores DNS.
7. Haga clic en **Guardar**.

Optimización de las conexiones de túnel seguras para dispositivos Android que utilizan aplicaciones de BlackBerry Dynamics

Si activa BlackBerry Secure Connect Plus y su entorno local incluye aplicaciones de BlackBerry Dynamics instaladas en dispositivos con Android Enterprise o dispositivos con Samsung Knox Workspace, se recomienda configurar el perfil de conectividad de BlackBerry Dynamics asignado a estos dispositivos para desactivar BlackBerry Proxy. El uso simultáneo de BlackBerry Proxy y BlackBerry Secure Connect Plus puede retrasar la actividad de la red de las aplicaciones porque los datos se enrutan a ambos componentes de la red.

1. En la barra de menú, haga clic en **Políticas y perfiles**.
2. Haga clic en **Redes y conexiones > Conectividad de BlackBerry Dynamics**.
3. Seleccione el perfil asignado a dispositivos Android Enterprise y Samsung Knox Workspace.
4. Haga clic en .
5. Desactive la casilla de verificación **Enrutar todo el tráfico**.
6. Haga clic en **Guardar**.

Resolución de problemas de BlackBerry Secure Connect Plus

Tenga en cuenta las cuestiones siguientes si tiene problemas para configurar BlackBerry Secure Connect Plus.

El adaptador de BlackBerry Secure Connect Plus entra en un estado de "Red no identificada" y deja de funcionar

Causa

Este problema puede ocurrir si reinicia el equipo que aloja BlackBerry Secure Connect Plus.

Solución: Windows Server 2012

1. En el Administrador del servidor, haga clic en **Administrar > Agregar funciones y características**. Haga clic en **Siguiente** hasta llegar a la pantalla **Características**. Expanda **Herramientas de administración de servidor remoto > Herramientas de administración de función** y seleccione **Herramientas de administración de acceso remoto**. Complete el asistente para instalar las herramientas.
2. Haga clic en **Herramientas > Administración de acceso remoto**.
3. En **Configuración**, haga clic en **DirectAccess y VPN**.
4. En **VPN**, haga clic en **Abrir administración de RRAS**.
5. Haga clic con el botón derecho en el servidor de enrutamiento y acceso remoto y en **Desactivar enrutamiento y acceso remoto**.
6. Haga clic con el botón derecho en el servidor de enrutamiento y acceso remoto y en **Configurar y activar enrutamiento y acceso remoto**.

7. Para completar el asistente de configuración, seleccione estas opciones:
   a. En la pantalla **Configuración**, seleccione **Traducción de direcciones de red (NAT)**.
   b. En la pantalla **Conexión a Internet de NAT**, seleccione **Usar esta interfaz pública para conectarse a Internet**. Compruebe que BlackBerry Secure Connect Plus se muestre en la lista de interfaces de red.
8. Abra **Enrutamiento y acceso remoto >** <*nombre del servidor*> **> IPv4** y haga clic en **NAT**. Abra las propiedades **Conexión de área local** y seleccione **Interfaz pública conectada a Internet** y **Activar NAT en este dispositivo**. Haga clic en **Aceptar**.
9. Abra las propiedades **BlackBerry Secure Connect Plus** y seleccione **Interfaz privada conectada a red privada**. Haga clic en **Aceptar**.
10. Haga clic con el botón derecho en el servidor de enrutamiento y acceso remoto y en **Todas las tareas > Reiniciar**.
11. En los servicios de Windows, reinicie el servicio **BlackBerry UEM: BlackBerry Secure Connect Plus**.

Descargue e instale la revisión del artículo KB de Windows La funcionalidad NAT falla en un servidor RRAS basado en Windows Server 2012.

BlackBerry Secure Connect Plus no se inicia

Causa posible

La configuración de TCP/IPv4 del adaptador de BlackBerry Secure Connect Plus podría no ser la correcto.

Solución posible

En **Conexiones de red > Adaptador de BlackBerry Secure Connect Plus > Propiedades > Protocolo de Internet versión 4 (TCP/IPv4) > Propiedades**, compruebe que **Utilizar la siguiente dirección IP** está activada, con los siguientes valores predeterminados:

- Dirección IP: 172.16.0.1
- Máscara de subred: 255.255.0.0

Si es necesario, corrija esta configuración y reinicie el servidor.

BlackBerry Secure Connect Plus deja de funcionar después de una instalación o actualización de BlackBerry UEM

Causa

Este problema puede ocurrir si el servidor no se reinició durante una actualización RRAS antes de actualizar BlackBerry UEM en un entorno local, lo que produce un error de configuración de enrutamiento/NAT durante la actualización. Este problema también puede producirse tras la nueva instalación de BlackBerry UEM.

Solución

1. Reinicie el servidor.
2. En los servicios de Windows, detenga el servicio **BlackBerry UEM: BlackBerry Secure Connect Plus**.
3. Como administrador, inicie Windows PowerShell (de 64 bits) o abra un símbolo del sistema.
4. Vaya a `<unidad>:\Archivos de programa\BlackBerry\UEMSecureConnectPlus\config\blackberry\` y ejecute **configureRRAS.bat**
5. Vaya a `<unidad>:\Archivos de programa\BlackBerry\UEMSecureConnectPlus\config\` y ejecute **configure-network-interface.cmd**

6. En los servicios de Windows, inicie el servicio **BlackBerry UEM: BlackBerry Secure Connect Plus**.

Presentación de los archivos de registro de BlackBerry Secure Connect Plus

Dos archivos de registro, ubicados de forma predeterminada en *<unidad>*:\Program Files\BlackBerry\UEM\Logs *<aaaammdd>* ,, registran datos acerca de BlackBerry Secure Connect Plus:

- BSCP: registra los datos sobre el componente del servidor de BlackBerry Secure Connect Plus
- BSCP-TS: registra los datos de registro para las conexiones con la aplicación BlackBerry Connectivity

En cada equipo que aloja una instancia de BlackBerry Connectivity Node, los archivos de registro de BlackBerry Secure Connect Plus se encuentran en *<unidad>*:\Program Files\BlackBerry\BlackBerry Connectivity Node\Logs *<aaaammdd>*.

Finalidad	Archivo de registro	Ejemplo
Compruebe que BlackBerry Secure Connect Plus esté conectado a BlackBerry Infrastructure	BSCP	2015-01-19T13:17:47.540-0500 - BSCP {TcpClientConnectorNio#2} logging.feature.bscp.service|logging.component.bscp.pss.bcp [{}] - DEBUG Received Ping from [id: 0x60bce5a3, /10.90.84.22:28231 => stratos.bcp.bblabs.rim.net/206.53.155.152:3101], responding with Pong.2015-01-19T13:18:22.989-0500 - BSCP {ChannelPinger#1} logging.feature.bscp.service|logging.component.bscp.pss.bcp [{}] - DEBUG Sending Ping to [id: 0xb4a1677a, /10.90.84.22:28232 => stratos.bcp.bblabs.rim.net/206.53.155.152:3101]
Compruebe que BlackBerry Secure Connect Plus esté preparado para recibir llamadas de la aplicación de BlackBerry Connectivity de los dispositivos	BSCP-TS	47: [14:13:21.231312][][3][AsioTurnSocket-1] Connected, host=68-171-243-141.rdns.blackberry.net 48: [14:13:21.239312][][3][AsioTurnSocket-1] Creating TURN allocation 49: [14:13:21.405121][][3][AsioTurnSocket-1] TURN allocation created
Compruebe que los dispositivos estén utilizando el túnel seguro	BSCP-TS	74: [10:39:45.746926][][3][Tunnel-2FFEC51E] Sent: 2130.6 KB (1733), Received: 201.9 KB (1370), Running: 00:07:00.139249
Compruebe que BlackBerry Secure Connect Plus esté utilizando la configuración del transcodificador personalizada	BSCP	"configuration_def" : "com.rim.p2e.vpn.server.cipherSuite" }], "TRANSCODER", ["provider", { "configuration_def" : "com.rim.p2e.vpn.transcoder.provider" }, "server_library", { "configuration_def" : "com.rim.p2e.vpn.transcoder.server.library" }, "server_config_blob", { "configuration_def" : "com.rim.p2e.vpn.transcoder.server.configBlob" }]]
Compruebe que los dispositivos estén utilizando un transcodificador personalizado	BSCP-TS	37: [13:41:39.800371][][3][BlackBerry_1.0.0.1-25B212A5] Connected

Uso de BlackBerry 2FA para establecer conexiones seguras a los recursos cruciales

BlackBerry 2FA protege el acceso a los recursos críticos de su empresa mediante la autenticación de dos factores. BlackBerry 2FA 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.

Usted administra BlackBerry 2FA desde la consola de administración de BlackBerry UEM, donde utiliza un perfil de BlackBerry 2FA para habilitar la autenticación de dos factores para sus usuarios. Para utilizar la versión más reciente de BlackBerry 2FA y sus características asociadas, tales como la autenticación previa y el autorrescate, sus usuarios deben tener el perfil de BlackBerry 2FA asignado. Para obtener más información, consulte el contenido de BlackBerry 2FA.

Configuración de la autenticación de registro único de los dispositivos

Puede activar los dispositivos con iOS para que realicen la autenticación automática en los dominios y servicios web de la red de su empresa. Después de asignar un perfil de registro único o un perfil de extensión de registro único, se le solicitará al usuario un nombre de usuario y contraseña la primera vez que intente acceder a un dominio seguro que haya especificado. La información de inicio de sesión se guarda en el dispositivo del usuario y se utiliza automáticamente cuando el usuario intenta acceder a cualquiera de los dominios seguros especificados en el perfil. Cuando el usuario cambia la contraseña, se le solicitará la próxima vez que intente acceder a un dominio seguro.

Para los dispositivos con iOS o iPadOS 13 o posterior, debe utilizar un perfil de extensión de registro único para permitir que los dispositivos se autentiquen automáticamente con los dominios y los servicios web de la red de su empresa. Los dispositivos que ejecuten una versión iOS anterior a 13 utilizaron perfiles de inicio de sesión único.

- Kerberos
- NTLM
- Certificados de SCEP para dominios de confianza especificados

Las aplicaciones de BlackBerry Dynamics también son compatibles con autenticación Kerberos. Para obtener más información, consulte Configuración de Kerberos para aplicaciones de BlackBerry Dynamics.

Creación de un perfil de extensión de registro único

Las extensiones de registro único son compatibles con los dispositivos con iOS y iPadOS 13 o posteriores. Puede especificar la configuración de una extensión personalizada o utilizar la extensión Kerberos proporcionada por Apple.

Antes de empezar: Si desea utilizar la autenticación basada en certificados, cree el perfil de certificado necesario.

1. En la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Redes y conexiones** > **Extensiones de registro único**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil.
5. En la lista desplegable **Tipo de extensión de registro único**, especifique si está utilizando una extensión personalizada o la extensión Kerberos proporcionada por Apple.

Tarea	Pasos
Si selecciona **Extensión personalizada**	**a.** En el campo **Identificador de extensión**, escriba el identificador de la aplicación que realiza el registro único. **b.** Especifique si el tipo de registro es **Credential** o **Redirigir** **c.** Si ha seleccionado **Credencial** como tipo de registro, realice los siguientes pasos: **1.** En el campo **Dominio**, escriba el nombre del dominio de las credenciales. **2.** En la sección **Dominios**, haga clic en + para añadir un dominio. **3.** En el campo **Nombre**, escriba el dominio para el que la extensión de la aplicación realizará el registro único. **4.** Añada dominios adicionales según sea necesario. **d.** Si ha seleccionado **Redirigir** como tipo de registro, realice los siguientes pasos: **1.** En la sección **URL**, haga clic en + para añadir una URL. **2.** En el campo **Nombre**, escriba el prefijo de la URL del proveedor de identidad para la que la extensión de la aplicación realizará el registro único. Añada URL adicionales según sea necesario. **e.** En el campo **Código de carga personalizado**, introduzca el código de carga personalizado para la extensión de la aplicación.

Tarea	Pasos
Si selecciona **Extensión integrada Kerberos**	**a.** En la sección **Dominios**, haga clic en + para añadir un dominio. **b.** En el campo **Nombre de dominio**, escriba el nombre del dominio de las credenciales. **c.** Seleccione los **datos de extensión de SSO de Apple Kerberos** adecuados para su entorno. De forma predeterminada, se permite el inicio de sesión automático y la detección automática de Active Directory. También puede especificar el dominio predeterminado, permitir que solo las aplicaciones gestionadas utilicen el registro único y requerir que los usuarios confirmen el acceso. **d.** Establezca el **Nombre principal** de la conexión. **e.** Si desea utilizar un perfil de certificado para proporcionar el certificado PKINIT para la autenticación, seleccione el tipo de perfil en la lista desplegable **Seleccionar el certificado PKINIT para la autenticación** y, a continuación, seleccione el perfil adecuado. **f.** Si está utilizando la API del servicio de seguridad genérico, especifique el **nombre de GSS de la caché Kerberos**. **g.** En la sección **Identificadores de paquetes de aplicaciones**, haga clic en + para especificar los ID de paquete que tienen permiso para acceder al ticket que concede el ticket. **h.** En la sección **Centros de distribución de claves preferidas**, haga clic en + para especificar los servidores preferidos si no son detectables mediante DNS. Especifique cada servidor en el mismo formato utilizado en un archivo krb5.conf. Los servidores especificados se utilizan para las comprobaciones de conectividad y se prueban primero para el tráfico de Kerberos. Si los servidores no responden, el dispositivo utiliza la detección de DNS. **i.** En el campo **Asignación de dominio-realm personalizada**, escriba cualquier asignación personalizada necesaria de nombres de dominios a realms en formato de carga útil, por ejemplo `<key>realm-ejemplo1</key><array><string>org</string></array>`. **j.** En el campo **Indicación de inicio de sesión**, especifique el texto que se mostrará en la parte inferior de la ventana de inicio de sesión de Kerberos .

6. Haga clic en **Guardar**.

Configuración de los perfiles de DNS para los dispositivos iOS y macOS

Puede especificar los servidores DNS que desea utilizar para acceder a dominios específicos. Esta configuración puede ayudar a proporcionar una experiencia de navegación web más rápida y segura en dispositivos que ejecutan iOS y iPadOS 14 y versiones posteriores y macOS 11 y versiones posteriores.

Creación de un perfil de DNS

1. En la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Redes y conexiones > DNS**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil.
5. Haga clic en la pestaña de un tipo de dispositivo.
6. Seleccione el protocolo DNS utilizado para comunicarse con el servidor DNS.
7. Lleve a cabo una de estas acciones:
   a) Si ha seleccionado **HTTPS**, escriba la plantilla de URI del servidor DNS sobre HTTPS mediante el esquema https://.
   b) Si ha seleccionado **TLS**, escriba el nombre de host del servidor DNS sobre TLS.
8. Seleccione la opción **No permitir que el usuario desactive la configuración de DNS** para evitar que los usuarios desactiven la configuración. Esta opción solo afecta a los dispositivos supervisados.
9. En el campo **Direcciones DNS**, especifique la lista de direcciones IP para los servidores DNS que desee utilizar. Pueden ser una combinación de direcciones IPv4 e IPv6.
10. En el campo **Dominios**, especifique la lista de cadenas de dominio que se deban utilizar para determinar qué consultas DNS utilizarán los servidores DNS.
11. En el campo **Reglas de DNS a petición**, especifique las reglas de DNS a petición utilizando el formato de carga de ejemplo.
12. Haga clic en **Guardar**.
13. Repita los pasos 5 a 12 para cualquier otro tipo de dispositivo.

Gestión del correo y de los dominios web para los dispositivos con iOS

Puede utilizar un perfil de dominios gestionados para definir determinados dominios de correo y dominios web como "dominios gestionados" que son internos a la empresa. Los perfiles de dominios gestionados solo se aplican a dispositivos con iOS y iPadOS con el tipo de activación de Controles de MDM.

Después de asignar un perfil de dominios gestionados:

- Cuando un usuario crea un mensaje de correo electrónico y agrega una dirección de correo electrónico del destinatario con un dominio que no está especificado en el perfil de dominios gestionados, el dispositivo muestra la dirección en color rojo para advertir al usuario de que el destinatario es externo a la empresa. El dispositivo no impedirá al usuario enviar correo a destinatarios externos.
- Un usuario debe usar una aplicación que se gestione mediante BlackBerry UEM para ver documentos desde un dominio web gestionado o documentos descargados desde un dominio web gestionado. El dispositivo no impide al usuario visitar o ver documentos desde otros dominios web. El perfil de dominios gestionados se aplica solamente al navegador Safari.

Creación de un perfil de dominios gestionados

Los perfiles de dominios gestionados se aplican únicamente a dispositivos con iOS y iPadOS.

1. En la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Redes y conexiones > Dominios gestionados**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil.
5. Opcionalmente, en el campo **Descripción**, escriba una descripción para el perfil.
6. En la sección **Dominios de correo electrónico gestionados**, haga clic en +.
7. En el campo **Dominios de correo electrónico**, escriba un nombre de dominio de nivel superior (por ejemplo, `ejemplo.com` en lugar de `ejemplo.com/canada`).
8. Haga clic en **Agregar**.
9. En la sección **Dominios web gestionados**, haga clic en +. Para ver ejemplos de formatos de dominio web, consulte Dominios web gestionados de Safari en la biblioteca del desarrollador de iOS.
10. En el campo **Dominios web**, escriba un nombre de dominio.
11. Si desea permitir que se rellene automáticamente la contraseña para los dominios web que ha especificado, seleccione la casilla de verificación **Permitir autorrelleno de la contraseña**. Esta opción solo es compatible con dispositivos supervisados.
12. Haga clic en **Agregar**.
13. Haga clic en **Agregar**.

Control del uso de la red de las aplicaciones de trabajo en los dispositivos iOS

Puede utilizar un perfil de uso de la red para controlar cómo utilizan la red móvil las aplicaciones de trabajo en los dispositivos que ejecutan iOS y iPadOS.

Para administrar el uso de la red, puede evitar que determinadas aplicaciones transfieran datos cuando los dispositivos están conectados a la red móvil o cuando los dispositivos están en roaming. Un perfil de uso de red puede contener reglas para una aplicación o para varias aplicaciones.

Creación de un perfil de uso de red

Las reglas de un perfil de uso de la red se aplican únicamente a aplicaciones de trabajo. Si no se han asignado las aplicaciones a los usuarios o a los grupos de usuarios, el perfil de uso de la red no tiene ningún efecto.

Antes de empezar: Agregue aplicaciones a la lista de aplicaciones y asígnelas a los grupos de usuarios o a las cuentas de usuario.

1. En la barra de menú, haga clic en **Políticas y perfiles**.
2. Haga clic en **Redes y conexiones > Uso de red**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil.
5. Haga clic en +.
6. Lleve a cabo una de las siguientes acciones:
   - Toque **Agregar una aplicación** y haga clic en una aplicación de la lista.
   - Seleccione **Especificar el ID de paquete de aplicación** y escriba el ID. El ID de paquete de aplicación también se conoce como ID de paquete. Puede encontrar el ID del paquete de aplicación haciendo clic en la aplicación que se encuentra en la lista de aplicaciones. Utilice un valor comodín (*) para que coincida con el ID de varias aplicaciones. (Por ejemplo, **com.company.***).
7. Para evitar que la aplicación o las aplicaciones utilicen datos cuando el dispositivo está en roaming, desactive la casilla de verificación **Permitir roaming de datos**.
8. Para evitar que la aplicación o las aplicaciones utilicen datos cuando el dispositivo está conectado a la red móvil, desactive la casilla de verificación **Permitir datos móviles**.
9. Haga clic en **Agregar**.
10. Repita los pasos 5 a 9 para cada aplicación que desee agregar a la lista.

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

Filtrado de contenido web en los dispositivos con iOS

Puede utilizar perfiles de filtro de contenido web para limitar los sitios web que un usuario puede ver en Safari o en otras aplicaciones de navegador en un dispositivo iOS o iPadOS supervisado. Se pueden asignar perfiles de filtro de contenido web a cuentas de usuarios, a grupos de usuarios y a grupos de dispositivos.

Al crear un perfil de filtro de contenido web, podrá elegir la opción de sitios web permitidos que admite los estándares de la empresa para el uso de dispositivos móviles.

Sitios web permitidos	Descripción
Solo sitios web específicos	En esta opción se permite solo el acceso a los sitios web que se especifiquen. Se crea un marcador en Safari para cada sitio web permitido. **Nota:** Si permite el acceso solo a sitios web específicos, debe asegurarse de que todos los sitios web a los que el dispositivo necesita acceder están especificados en la lista de sitios web permitidos. Por ejemplo, si configura la autenticación moderna de Microsoft Office 365 para las aplicaciones de BlackBerry Dynamics, el dispositivo debe poder acceder al sitio web de los servicios de federación de Active Directory.
Limitar contenido para adultos	Esta opción activa el filtrado automático para identificar y bloquear contenido inapropiado. También puede incluir sitios web específicos utilizando los siguientes ajustes: • URL permitidas: puede agregar una o más direcciones URL para permitir el acceso a sitios web específicos. Los usuarios pueden ver sitios web de esta lista, independientemente de si el filtrado automático bloquea el acceso. • URL en la lista negra: puede agregar una o más direcciones URL para permitir el acceso a sitios web específicos. Los usuarios no pueden ver sitios web de esta lista, independientemente de si el filtrado automático permite el acceso.

Creación de un perfil de filtro de contenido web

Cuando se crea un perfil de filtro de contenido web, cada una de las URL que especifique debe comenzar con http:// o https://. Si es necesario, debe agregar entradas separadas para las versiones http:// o https:// de la misma URL. La resolución de DNS no se produce, por lo tanto, los sitios web de acceso restringido aún podrían ser accesibles (por ejemplo, si especifica http://www.example.com los usuarios pueden acceder a la web utilizando la dirección IP).

1. En la barra de menú, haga clic en **Políticas y perfiles**.
2. Haga clic en **Redes y conexiones > Filtro de contenido web**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil de filtro de contenido web.
5. Lleve a cabo una de las tareas siguientes:

Tarea	Pasos
Permitir el acceso solo a sitios web específicos	**a.** En la lista desplegable **Sitios web permitidos**, compruebe que esté seleccionada la opción **Solo sitios web específicos**. **b.** En la sección **Sitios web favoritos específicos**, haga clic en +. **c.** Realice las acciones siguientes: **1.** En el campo **URL**, escriba la dirección web para la que desea permitir el acceso. **2.** Opcionalmente, en el campo **Ruta de favoritos**, escriba el nombre de una carpeta de favoritos (por ejemplo, /Trabajo/). **3.** En el campo **Título**, escriba un nombre para el sitio web. **4.** Haga clic en **Agregar**. **d.** Repetir los pasos 2 y 3 para cada sitio web permitido.
Limitar contenido para adultos	**a.** En la lista desplegable **Sitios web permitidos**, haga clic en **Limitar contenido para adultos** para activar el filtrado automático. **b.** Opcionalmente, lleve a cabo las acciones siguientes: **1.** Haga clic en + al lado de **URL permitidas**. **2.** Escriba la dirección web para la que desea permitir el acceso. **3.** Repetir los pasos 2.a y 2.b para cada sitio web permitido. **c.** Opcionalmente, lleve a cabo las acciones siguientes: **1.** Haga clic en + al lado de **URL en la lista negra**. **2.** Escriba la dirección web para la que desea denegar el acceso. **3.** Repetir los pasos 3.a y 3.b para cada sitio web restringido.

6. Haga clic en **Agregar**.

Configuración de perfiles de AirPrint y AirPlay para dispositivos iOS

Los perfiles de AirPrint pueden ayudar a los usuarios a encontrar impresoras que sean compatibles con AirPrint, a las que sea fácil acceder y para las que tengan los permisos necesarios. En las situaciones en las que los protocolos como Bonjour no pueden detectar impresoras con AirPrint en otra subred, los perfiles de AirPrint ayudan a especificar el lugar en el que se encuentran los recursos. Puede asignar perfiles de AirPrint a los dispositivos con iOS y iPadOS para que los usuarios no tengan que configurar las impresoras manualmente.

AirPlay es una función que permite mostrar fotos o transmitir música y vídeo a dispositivos AirPlay compatibles, tales como Apple TV, AirPort Express, o altavoces habilitados para AirPlay.

Con un perfil de AirPlay puede especificar a qué dispositivos AirPlay se pueden conectar los usuarios de iOS y iPadOS. El perfil de AirPlay tiene dos opciones:

- Si los dispositivos AirPlay de su empresa están protegidos por contraseña, puede especificar las contraseñas de los dispositivos de destino permitidos para que los usuarios de dispositivos iOS y iPadOS puedan conectarse sin conocer la contraseña.
- En el caso de los dispositivos supervisados, puede restringir a qué dispositivos AirPlay pueden conectarse los usuarios elaborando una lista de dispositivos AirPlay permitidos para los dispositivos supervisados. Los dispositivos supervisados solo se pueden conectar a los dispositivos AirPlay especificados en la lista. Si no crea una lista, los dispositivos supervisados podrán conectarse a cualquier dispositivo AirPlay.

Creación de un perfil de AirPrint

Puede configurar perfiles de AirPrint y asignarlos a los dispositivos iOS y iPadOS para que los usuarios no tengan que configurar las impresoras manualmente.

Para obtener más información sobre el protocolo Bonjour y la impresión con una aplicación de BlackBerry Dynamics, visite support.blackberry.com/community para consultar el artículo 40030.

1. En la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Redes y conexiones > AirPrint**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil de AirPrint.
5. En la sección **Configuración de AirPrint**, haga clic en +.
6. En el campo **Dirección IP**, escriba la dirección IP de la impresora o del servidor de AirPrint.
7. En el campo **Ruta del recurso**, escriba la ruta del recurso de la impresora.
   La ruta del recurso de la impresora corresponde al parámetro `rp` del registro `_ipps.tcp` Bonjour. Por ejemplo:
   - printers/<*series de impresoras*>
   - printers/<*modelo de impresora*>
   - ipp/print
   - IPP_Printer
8. Opcionalmente, si las conexiones de AirPrint están protegidas mediante TLS, seleccione la casilla de verificación **Forzar TLS**.
9. Opcionalmente, si el puerto difiere del predeterminado por el protocolo de impresión de Internet, escriba el número de puerto en el campo **Puerto**.
10. Haga clic en **Agregar**.

11. Haga clic en **Agregar**.

Creación de un perfil de AirPlay

1. En la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Redes y conexiones > AirPlay**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil de AirPlay.
5. Haga clic en + en la sección **Dispositivos de destino permitidos**.
6. En el campo **Nombre del dispositivo**, escriba el nombre del dispositivo AirPlay que desea agregar. Puede encontrar el nombre del dispositivo AirPlay en los ajustes del dispositivo o puede buscar el nombre del dispositivo tocando **AirPlay** en el Centro de Control de un dispositivo iOS o iPadOS para ver una lista de dispositivos AirPlay disponibles cerca.
7. En el campo **Contraseña**, escriba la contraseña correcta.
8. Haga clic en **Agregar**.
9. Haga clic en + en la sección **Dispositivos de destino permitidos para los dispositivos supervisados**.
10. En el campo **ID del dispositivo**, escriba el ID de dispositivo AirPlay al que desea permitir conectarse a los dispositivos. Puede encontrar el ID del dispositivo AirPlay en los ajustes del dispositivo. Los dispositivos supervisados solo se pueden conectar a dispositivos AirPlay de la lista.
11. Haga clic en **Agregar**.

Configuración de nombres de punto de acceso para dispositivos Android

Un APN especifica la información que necesita un dispositivo móvil para conectarse a una red del operador. Puede utilizar uno o más perfiles de nombre de punto de acceso para enviar APN de operadores a los dispositivos Android de los usuarios. Los perfiles de nombre de punto de acceso son compatibles con los dispositivos Android 9 y posteriores con activaciones de Solo espacio de trabajo y dispositivos Android 9 y 10 con activaciones de Trabajo y personal: control total.

Los dispositivos suelen tener APN preestablecidos para los operadores comunes. Los usuarios también pueden añadir APN nuevos a un dispositivo. Si quiere forzar que un dispositivo utilice un APN que se le ha enviado mediante un perfil de nombre de punto de acceso, seleccione la regla de política de TI "Fuerce al dispositivo a usar el nombre del punto acceso en los ajustes de perfil" en las reglas de políticas de TI Android global (todos los dispositivos Android).

Creación de un perfil de nombre de punto de acceso

Antes de empezar: Obtenga la configuración de APN necesaria del operador.

1. En la barra de menú, haga clic en **Políticas y perfiles**.
2. Haga clic en **Redes y conexiones > Nombre de punto de acceso**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil de nombre de punto de acceso. Dicha información se muestra en los dispositivos.
5. Escriba el **Nombre de punto de acceso**.
6. Indique los valores que coincidan con las especificaciones del operador de cada configuración de perfil.
   Para obtener más información, consulte Configuración del perfil de nombre de punto de acceso.
7. Haga clic en **Guardar**.

Configuración del perfil de nombre de punto de acceso

Configuración del perfil de nombre de punto de acceso	Descripción
Nombre de punto de acceso	En esta configuración se especifica el nombre de punto de acceso (APN) que debe utilizar su dispositivo cuando se comunica con el operador. El APN es una breve cadena de texto.

Configuración del perfil de nombre de punto de acceso	Descripción
Máscara de bits de tipo de APN	Esta configuración especifica los tipos de comunicación de datos que utiliza esta configuración de APN. Los distintos tipos de comunicaciones pueden utilizar diferentes configuraciones. Valores posibles: • Tráfico de datos predeterminado • Tráfico MMS • GPS asistido por SUPL • Tráfico DUN • Tráfico de prioridad alta • Acceder al portal FOTA del operador • IMS • CBS • APN de conexión inicial IA • PDN de emergencia • MCX (servicio fundamental)
Dirección del proxy	En esta configuración se especifica el proxy HTTP que se utilizará para todo el tráfico web que se produzca a través de la conexión. Esta configuración no es necesaria para la mayoría de los operadores.
Puerto de proxy	En esta configuración se especifica el puerto del proxy HTTP que se utilizará para todo el tráfico web que se produzca a través de la conexión. Esta configuración no es necesaria para la mayoría de los operadores.
MMSC	En esta configuración se especifica el centro de servicios de mensajería multimedia (MMSC) que se utilizará para enviar y recibir mensajes MMS.
Dirección del proxy MMS	En esta configuración se especifica el proxy HTTP para la comunicación con el MMSC para enviar y recibir mensajes MMS.
Puerto del proxy MMS	En esta configuración se especifica el puerto del proxy HTTP para la comunicación con el MMSC para enviar y recibir mensajes MMS.
Tipo de autenticación	En esta configuración se especifica el tipo autenticación que utiliza en las comunicaciones. Valores posibles: • NINGUNO • PAP • CHAP • PAP o CHAP
Nombre de usuario	Si la configuración "Tipo de autenticación" se establece en un valor distinto de NINGUNO, especifique un nombre de usuario si es necesario para la autenticación.

Configuración del perfil de nombre de punto de acceso	Descripción
Contraseña	Si la configuración "Tipo de autenticación" se establece en un valor distinto de NINGUNO, especifique una contraseña si es necesario para la autenticación.
Código de país móvil (MCC)	En esta configuración se especifica el código de país móvil de la red del operador para la que debe utilizarse la configuración de APN.
Código de red móvil (MNC)	En esta configuración se especifica el código de red móvil de la red del operador para la que debe utilizarse la configuración de APN.
Protocolo	En esta configuración se especifica si se debe habilitar IPv4, IPv6 o ambas opciones en la red doméstica para los dispositivos que admiten redes IPv6. Valores posibles: • IP • IPv6 • IPv4v6 • PPP
Protocolo de itinerancia	En esta configuración se especifica si se debe habilitar IPv4, IPv6 o ambas opciones en itinerancia para los dispositivos que admiten redes IPv6. Valores posibles: • IP • IPv6 • IPv4v6 • PPP
Operador activado	En esta configuración se especifica si el APN está activado para el operador.
Tipo de OMV	En esta configuración se especifica si se restringe el uso de este APN a MVNO (distribuidores de redes móviles) o cuentas de suscriptor determinados. Valores posibles: • SP • IMSI • GID • ICCID

Aviso legal

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

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

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

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

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

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

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

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

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

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

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

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

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

Publicado en Canadá