BlackBerry UEM

Gestión de conexiones seguras

12.20

Contents

Gestión de conexiones seguras con BlackBerry UEM

La siguiente tabla muestra un resumen de las tareas de administración incluidas en esta guía. Revísela para determinar qué tareas debe completar en función de las necesidades de su empresa.

Tarea	Descripción
Crear un perfil de Wi-Fi	Puede crear un perfil de Wi-Fi para especificar cómo los dispositivos se conectan a una red Wi-Fi de trabajo.
Crear un perfil de VPN	Puede crear un perfil de VPN para especificar cómo los dispositivos se conectan a una VPN de trabajo.
Crear un perfil de VNP por aplicación	Puede especificar qué aplicaciones de los dispositivos deben utilizar una VPN para los datos en tránsito.
Crear un perfil de proxy	Puede especificar cómo los dispositivos utilizan un servidor proxy para acceder a servicios web en Internet o en una red de trabajo.
Creación de un perfil de conectividad de la empresa	Puede especificar cómo se conectan los dispositivos a los recursos de su empresa mediante la conectividad de la empresa y BlackBerry Secure Connect Plus para proporcionar un túnel IP seguro entre las aplicaciones y la red de su empresa.
Crear un perfil de BlackBerry 2FA	Puede habilitar la autenticación de dos factores para los usuarios y especificar la configuración de las funciones de preautenticación y autorrescate.
Creación de un perfil de extensión de registro único	Puede activar los dispositivos con iOS y iPadOS para que realicen la autenticación automática en los dominios y servicios web de la red de su empresa.
Crear un perfil de conectividad de BlackBerry Dynamics	Puede definir 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. Para obtener más información, consulte Configuración de conexiones de red para aplicaciones de BlackBerry Dynamics en el contenido de Administración.
Creación de un perfil de DNS	Puede especificar los servidores DNS que desea que utilicen los dispositivos iOS y macOS para acceder a los dominios especificados.
Crear un perfil de correo electrónico	Puede especificar cómo se conectan los dispositivos a un servidor de correo de trabajo y cómo sincronizan los mensajes de correo electrónico, las entradas del calendario y los datos del organizador mediante Exchange ActiveSync o IBM Notes Traveler. Para obtener más información, consulte Creación de perfiles de correo electrónico en el contenido de Administración.
Creación de un perfil de correo IMAP/POP3	Puede especificar cómo se conectan los dispositivos a un servidor de correo IMAP o POP3 y sincronizan los mensajes de correo. Para obtener más información, consulte Creación de un perfil de correo iIMAP/POP3 en el contenido de Administración.

Tarea	Descripción
Creación de un perfil de uso de red	Puede administrar el uso de la red móvil de las aplicaciones iOS y iPadOS.
Creación de un perfil de filtro de contenido web	Puede limitar los sitios web que un usuario puede ver en Safari o en otros navegadores en un dispositivo iOS o iPadOS supervisado.
Creación de un perfil de AirPrint	Puede ayudar a los usuarios a encontrar impresoras.
Creación de un perfil de AirPlay	Puede especificar a qué dispositivos AirPlay se pueden conectar los usuarios de iOS y iPadOS.
Creación de un perfil de nombre de punto de acceso	Puede especificar la información que necesitan los dispositivos Android para comunicarse con la red del operador.
Conexión de UEM al software de PKI de la empresa	Puede ampliar la autenticación basada en certificados que proporcionan los servicios de PKI a los dispositivos y aplicaciones que administra con UEM. Por ejemplo, puede • Conexión de BlackBerry UEM al software de Entrust de la empresa • Conectar BlackBerry UEM al servidor de Entrust IdentityGuard de su empresa para utilizar credenciales inteligentes • Conexión de BlackBerry UEM al software de OpenTrust de la empresa • Conexión de BlackBerry UEM a un conector PKI de BlackBerry Dynamics • Conexión de BlackBerry UEM a la solución PKI basada en aplicación de su empresa
Enviar certificados a dispositivos y aplicaciones mediante perfiles	Puede enviar certificados a dispositivos y aplicaciones utilizando perfiles de UEM.
Administrar certificados de cliente para cuentas de usuario	Puede agregar certificados de cliente directamente a cuentas de usuarios individuales o a un perfil de credenciales de usuario asignado a la cuenta de este.

Administración de las conexiones de trabajo mediante los perfiles

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.

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. Por ejemplo, puede asociar perfiles de certificado y perfiles 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 protegida por el firewall. Se puede asignar un perfil de Wi-Fi a cuentas de usuarios, grupos de usuarios o grupos de dispositivos.

De forma predeterminada, tanto las aplicaciones de trabajo como las personales pueden utilizar los perfiles de Wi-Fi 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. 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.

Antes de empezar:

- Si los dispositivos utilizan la autenticación basada en certificados para las conexiones Wi-Fi de trabajo, cree un perfil de certificado de CA y asígnelo a las cuentas de usuario, los grupos de usuarios o 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 de Wi-Fi.
- 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 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. Haga clic en la pestaña de un tipo de dispositivo para configurar los valores adecuados. Para obtener más información, consulte la configuración del perfil Wi-Fi para iOS y macOS, Android y Windows.

   Si su empresa requiere que los usuarios proporcionen un nombre de usuario y una contraseña para conectarse a la red Wi-Fi, en el campo **Nombre de usuario**, escriba `%UserName%`.
8. Repita el paso 7 para cada tipo de dispositivo.
9. Haga clic en **Agregar**.

Después de terminar: Asigne el perfil Wi-Fi a cuentas de usuarios, grupos de usuarios o grupos de dispositivos.

iOS y macOS: configuración de perfil Wi-Fi

iOS, iPadOS y macOS: configuración de perfil Wi-Fi	Descripción
Aplicar perfil a	En esta configuración se especifica si el perfil Wi-Fi de un dispositivo con macOS se aplica a la cuenta de usuario o al dispositivo.
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 cuando se conectan a la red Wi-Fi.
Perfil proxy asociado	En la configuración se especifica el perfil de proxy asociado que un dispositivo utiliza para conectarse al servidor proxy cuando el dispositivo se conecta a la red Wi-Fi.
Tipo de red	Esta configuración especifica la configuración para la red Wi-Fi. Las configuraciones del punto de acceso se aplican únicamente a dispositivos macOS, iOS y iPadOS. 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.
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.

iOS, iPadOS y macOS: configuración de perfil Wi-Fi	Descripción
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".
Tipo de seguridad	En la configuración se 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".
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, iPadOS y macOS: configuración de perfil Wi-Fi	Descripción
Protocolo de autenticación	En la configuración se especifican los métodos EAP que admite 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".
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".
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".
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	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 con WEP", "WPA-Enterprise", "WPA2-Enterprise" o "WPA3-Enterprise".

iOS, iPadOS y macOS: configuración de perfil Wi-Fi	Descripción
Contraseña	En esta configuración se especifica la contraseña que utiliza un dispositivo para la autenticación en 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 esta configuración se especifica el nombre de usuario que utiliza un dispositivo para la autenticación en 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	En esta configuración se especifica el tipo de autenticación que utiliza un dispositivo 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".
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".
Perfil de certificado compartido	En esta configuración se especifica el perfil de certificado compartido con el certificado de cliente que utiliza un dispositivo para la autenticación en 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	En esta configuración se especifica el nombre del certificado de cliente que utiliza un dispositivo para la autenticación en 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	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. Esta configuración es válida únicamente si la opción "Tipo de autenticación" se establece en "SCEP".

iOS, iPadOS y macOS: configuración de perfil Wi-Fi	Descripción
Perfil de credenciales de usuario asociado	En esta configuración se especifica el perfil de credenciales de usuario asociado que utiliza un dispositivo para obtener un certificado de cliente para la autenticación en 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".
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 con WEP", "WPA-Enterprise", "WPA2-Enterprise" o "WPA3-Enterprise".
Perfiles de certificado de CA	En esta configuración se especifican los perfiles de certificado de CA con los certificados de confianza que utiliza 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	En esta configuración se especifica el nombre de los certificados de confianza que utiliza 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 "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.

iOS, iPadOS y macOS: configuración de perfil Wi-Fi	Descripción
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: ajuste del perfil de Wi-Fi	Descripción
Perfil proxy asociado	En esta configuración se especifica el perfil de proxy asociado que utilizan los dispositivos Android para conectarse al servidor proxy cuando el dispositivo está conectado a la red Wi-Fi. Los dispositivos Android con activaciones Controles de MDM o Privacidad del usuario no son compatibles con los perfiles de Wi-Fi con configuración de proxy.
BSSID	En la 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.
Tipo de seguridad personal	En la configuración se especifica el tipo de seguridad personal que debe utilizar la red Wi-Fi. Esta configuración es válida únicamente si la opción "Tipo de seguridad" se establece en "Personal".

Android: ajuste 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 la configuración se especifica el método EAP que debe utilizar la red Wi-Fi. Esta configuración es válida únicamente si la opción "Tipo de seguridad" se establece en "Empresa". LEAP no es compatible con los dispositivos que utilizan Samsung Knox.
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". CHAP no es compatible con los dispositivos que utilizan Samsung Knox.
Identidad externa de TTLS	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".
Identidad externa de PEAP	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 "PEAP".

Android: ajuste del perfil de Wi-Fi	Descripción
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 la configuración se especifica el tipo de autenticación que un dispositivo Android debe utilizar para conectarse a la red Wi-Fi. Esta configuración es válida únicamente si la opción "Tipo de seguridad" se establece en "Empresa".
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".
Perfil de certificado compartido	En la configuración se especifica el perfil de certificado compartido con el certificado de cliente que un dispositivo Android debe utilizar para autenticar 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 la configuración se especifica el perfil SCEP asociado que un dispositivo Android 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". El nombre del perfil SCEP debe tener menos de 36 caracteres para los dispositivos que utilizan un Knox Workspace.

Android: ajuste del perfil de Wi-Fi	Descripción
Perfil de credenciales de usuario asociado	En la configuración se especifica el perfil de credenciales de usuario asociado que un dispositivo Android 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 "Credenciales del usuario". El nombre del perfil de credenciales de usuario debe tener menos de 36 caracteres para los dispositivos que utilizan un Knox Workspace.
Nombre del certificado de cliente	En la configuración se especifica el nombre del certificado de cliente que un dispositivo Android debe utilizar para autenticar 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	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".
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".
Perfil de certificado de CA	En la configuración se especifica el perfil de certificado de CA con el certificado de confianza que un dispositivo Android 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 "Referencia única".
Nombres de certificados de confianza	En la configuración se especifica el nombre de los certificados de confianza que un dispositivo Android 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".

Windows: configuración del perfil de Wi-Fi

Windows: ajuste 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.

Windows: ajuste del perfil de Wi-Fi	Descripción
Tipo de seguridad	En la configuración se especifica el tipo de seguridad que utiliza la red Wi-Fi.
Tipo de cifrado	En este ajuste 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.
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".
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".
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", el registro único se realizará antes de que el usuario inicie sesión en Active Directory. Si se establece en "Realizar inmediatamente después del inicio de sesión del usuario", el registro único se realizará inmediatamente después de que el usuario inicie sesión en Active Directory. Esta configuración solo es válida si se ha seleccionado la opción "Activar registro único".
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".

Windows: ajuste del perfil de Wi-Fi	Descripción
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".
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".

Windows: ajuste del perfil de Wi-Fi	Descripción
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 estado 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 almacenar en la caché la PMK para activar el 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".
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".
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".
Esta red utiliza la autenticación previa	Este ajuste especifica si el punto de acceso es compatible con la autenticación previa del roaming rápido 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".

Windows: ajuste del perfil de Wi-Fi	Descripción
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.
Tipo de proxy	Esta configuración especifica el tipo de configuración de proxy para el perfil Wi-Fi. La configuración se aplica únicamente a dispositivos Windows 10 Mobile.
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".
Desactivar comprobaciones de conectividad a Internet	En la configuración se especifica si desea desactivar las comprobaciones de conectividad a Internet.
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 conectarse a una VPN de trabajo para dispositivos Android que no sean Samsung Knox, puede configurar los ajustes de VPN utilizando los ajustes de configuración de 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. Debe instalar una aplicación de cliente VPN compatible que utilice KNOX SDK en el dispositivo.
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.

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

Crear un perfil VPN

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. 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.

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

Antes de empezar:

- Si los dispositivos utilizan la autenticación basada en certificados para las 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 SCEP, un certificado compartido o un perfil de credenciales de usuario 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.

- 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. Haga clic en la pestaña de un tipo de dispositivo para configurar los valores adecuados. Para obtener más información, consulte la configuración del perfil de VPN para iOS y macOS, Android y Windows.

   Si la empresa requiere que los usuarios proporcionen un nombre de usuario y una contraseña para conectarse a la red de VPN, en el campo **Nombre de usuario**, escriba `%UserName%`.
6. Haga clic en **Agregar**.

Después de terminar: Asigne el perfil Wi-Fi a cuentas de usuarios, grupos de usuarios o grupos de dispositivos.

iOS y macOS: configuración del perfil de VPN

iOS, iPadOS y macOS: configuración del perfil de VPN	Descripción
Aplicar perfil a	Esta configuración especifica si el perfil de VPN de un dispositivo macOS se aplica a la cuenta de usuario o al dispositivo.
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. Si selecciona "IKEv2 siempre activado", muchos ajustes tienen valores independientes para la red móvil y las conexiones Wi-Fi.
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, iPadOS y macOS: configuración del perfil de VPN	Descripción
Dominio o grupo de inicio de sesión	Esta configuración especifica el dominio o grupo de inicio de sesión que la puerta de enlace VPN utiliza para autenticar un dispositivo. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "SonicWALL Mobile Connect".
Alcance	Esta configuración especifica el nombre del dominio de autenticación que la puerta de enlace VPN utiliza para autenticar un dispositivo. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "Juniper" o "Pulse Secure."
Cargo	Esta configuración especifica el nombre del rol de usuario que la puerta de enlace VPN utiliza 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.
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".
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".

iOS, iPadOS y macOS: configuración del perfil de VPN	Descripción
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	Esta configuración especifica el perfil SCEP asociado que un dispositivo utiliza 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".
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".
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"

iOS, iPadOS y macOS: configuración del perfil de VPN	Descripción
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	En la configuración se 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".
ID remoto	En la configuración se 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 los dispositivos 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".

iOS, iPadOS y macOS: configuración del perfil de VPN	Descripción
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".
Desconectar por inactividad del temporizador	Esta configuración especifica el tiempo de inactividad en segundos tras el que debe desconectarse la VPN. 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 "Personalizado".
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.
Todas las rutas no predeterminadas tienen prioridad sobre cualquier ruta definida localmente	Esta configuración 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 "Personalizado".
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 a los dispositivos con iOS y iPadOS 13 y versiones posteriores.

iOS, iPadOS y macOS: configuración del perfil de VPN	Descripción
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 "Personalizado".
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 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".
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".
Tipo de certificado	Esta configuración especifica el tipo de certificado que se utiliza 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".
Nombre común del emisor del certificado de servidor	Esta configuración especifica el nombre común de la CA que emitió el certificado de servidor que el servidor IKE envía al dispositivo. Esta configuración es obligatoria si se activa xAuth mediante un certificado. Esta configuración es válida únicamente si se selecciona la opción "Activar xAuth" y el Tipo de autenticación es "Certificado".

iOS, iPadOS y macOS: configuración del perfil de VPN	Descripción
Nombre común del certificado de servidor	Esta configuración especifica el nombre común del certificado del servidor que el servidor IKE envía 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".
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".
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".
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".

iOS, iPadOS y macOS: configuración del perfil de VPN	Descripción
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".
MTU	Esta configuración especifica la Unidad de transmisión máxima en bytes. Esta configuración es válida únicamente si la opción "Tipo de conexión" se establece en "IKEv2 siempre activado".
Mensaje de voz	Esta configuración 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 es válida únicamente si la opción "Tipo de conexión" se establece en "IKEv2 siempre activado". Solo se aplica a las conexiones Wi-Fi.

iOS, iPadOS y macOS: configuración del perfil de VPN	Descripción
AirPrint	Esta configuración especifica si las conexiones de AirPrint se envían a través del túnel VPN, se envían fuera del túnel VPN o se bloquean. 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 especifica si el tráfico de hojas web 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 especifica si el tráfico de todas las aplicaciones de red cautivas se puede enviar fuera del túnel VPN. Si no se selecciona esta configuración, 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	Esta configuración especifican las aplicaciones de red 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	Esta configuración 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.
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.
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.
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.

iOS, iPadOS y macOS: configuración del perfil de VPN	Descripción
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.
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", "Personalizado", "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 los dominios que pueden iniciar la conexión VPN en Safari. Esta configuración es válida únicamente si se ha seleccionado la opción "Activar VPN por aplicación".
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".
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".
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".

iOS, iPadOS y macOS: configuración del perfil de VPN	Descripción
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".
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".
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".
Perfil proxy asociado	Esta configuración especifica el perfil de proxy asociado que un dispositivo utiliza para conectarse a un 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 con 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. 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".

Android: configuración del perfil de VPN	Descripción
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. Si el ajuste "Tipo de VPN" se establece en "IPsec", este ajuste se debe establecer en "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".
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. 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. 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. 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".
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".

Android: configuración del perfil de VPN	Descripción
Modo de intercambio de clave IKE fase 1	En la configuración se especifica el modo de intercambio para VPN. 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. 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".
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".

Android: configuración del perfil de VPN	Descripción
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. 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".
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.
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.
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.

Android: configuración del perfil de VPN	Descripción
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.
Conectividad de la empresa para dispositivos Android con un espacio de trabajo	Esta configuración especifica si los dispositivos Samsung Knox 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 del perfil de VPN

Windows: configuración del perfil de VPN	Descripción
Tipo de conexión	En esta configuración se especifica el tipo de conexión que utiliza un dispositivo Windows 10 para una VPN.
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".
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".

Windows: configuración del perfil de VPN	Descripción
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".
Tipo de protocolo integrado	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".
Autenticación	En la configuración se especifica el método de autenticación utilizado para la VPN nativa. La configuración "Tipo de protocolo integrado" determina qué métodos de autenticación son compatibles y el valor predeterminado de esta configuración.
Configuración de EAP	Este ajuste especifica el valor XML de la configuración de EAP. 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".
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".
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 del perfil de 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`. • 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 del perfil de 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`. • 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.
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.
Recordar credenciales	En la configuración se especifica si las credenciales se almacenan en caché siempre que sea posible.
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.

Windows: configuración del perfil de VPN	Descripción
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	Esta configuración especifica el nivel de autenticación de una VPN. Esta configuración debe coincidir con la del servidor VPN.
Constantes de transformación de cifrado	Esta configuración especifica el nivel de cifrado de una VPN. Esta configuración debe coincidir con la del servidor VPN.
Método de cifrado	Esta configuración especifica el nivel de cifrado de fase 1 de una VPN. Esta configuración debe coincidir con la del servidor VPN.
Método de comprobación de integridad	Esta configuración especifica el nivel de autenticación de fase 1 de una VPN. Esta configuración debe coincidir con la del servidor VPN.
Grupo Diffie-Hellman	Esta configuración especifica el grupo de claves de una VPN. Esta configuración debe coincidir con la del servidor VPN.
Grupo PFS	Esta configuración especifica el protocolo de cifrado de confidencialidad directa perfecta que se utiliza para la VPN. Esta configuración debe coincidir con la del servidor VPN.
Tipo de proxy	Esta configuración especifica el tipo de configuración de proxy para la VPN.
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 .

Integración de BlackBerry UEM con CylanceGATEWAY para crear un perfil ZTNA

Como alternativa al uso de un perfil VPN, puede integrar su UEM con CylanceGATEWAY. CylanceGATEWAY es una solución de acceso a la red de confianza cero (ZTNA) nativa de la nube y asistida por inteligencia artificial (IA) que puede habilitarse para su inquilino de Cylance Endpoint Security. A continuación, puede configurar CylanceGATEWAY en la consola de administración de Cylance. Para obtener más información sobre cómo configurar CylanceGATEWAY, consulte Configuración de BlackBerry Gateway en el contenido de configuración

de Cylance Endpoint Security. 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 y 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.

Activación y asignación de ajustes de VPN por aplicación

Puede configurar una VPN por aplicación en los dispositivos con iOS, iPadOS, Samsung Knox y Windows 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.

Dispositivos	Ajustes de aplicaciones
iOS y iPadOS	Las aplicaciones se asocian a un perfil de VPN cuando se asigna la aplicación o el grupo de aplicaciones a un usuario, un grupo de usuarios o un grupo de dispositivos.
Dispositivos Samsung Knox con Android Enterprise y activaciones de Samsung Knox Workspace	Las aplicaciones se añaden a la configuración "Aplicaciones que pueden utilizar la conexión VPN" en el perfil de VPN.
Windows 10	Las aplicaciones se añaden a la configuración "Lista de activadores de la aplicación" en el perfil de VPN.

Solo se puede asignar un perfil de VPN a una aplicación o grupo de aplicaciones.

BlackBerry UEM utiliza las siguientes reglas para determinar la configuración de VPN por aplicación que se debe asignar a una aplicación en los dispositivos iOS y iPadOS:

Configuración de VPN por aplicación	Prioridad
Si se asocia directamente a una aplicación	Tiene prioridad sobre la configuración de VPN por aplicación asociada indirectamente por un grupo de aplicaciones.

Configuración de VPN por aplicación	Prioridad
Si se asocia directamente a un usuario	Tiene prioridad sobre la configuración de VPN por aplicación asociada indirectamente por un grupo de usuarios.
Si se asigna a una aplicación necesaria	Tiene prioridad sobre la configuración de VPN por aplicación asignada a una instancia opcional de la misma aplicación.
Si se asocia con el nombre del grupo de usuarios que aparece anteriormente en la lista alfabética	Tiene 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 autenticación.

Dispositivo	Configuración de proxy
iOS y iPadOS	Cree un perfil de proxy y asócielo a un perfil Wi-Fi o de VPN. Puede asignar un perfil de proxy a cuentas de usuarios, grupos de usuarios y grupos de dispositivos. 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-Fi o de VPN. macOS aplica perfiles a las cuentas de usuario o los dispositivos. Los perfiles de proxy se aplican a los dispositivos.

Dispositivo	Configuración de proxy
Android	Para dispositivos con Android Enterprise, cree un perfil de proxy y asócielo a un perfil de Wi-Fi. Los dispositivos Android con activaciones Controles de MDM o Privacidad del usuario no son compatibles con los perfiles de Wi-Fi con configuración de proxy.
Samsung Knox	Cree un perfil de proxy y asócielo a un perfil de Wi-Fi, VPN o conectividad de 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 con Samsung Knox con activaciones de Android Enterprise y los dispositivos con Knox Workspace que utilizan una versión de Knox posterior a 2.5. Puede asignar un perfil de proxy a cuentas de usuarios, grupos de usuarios y 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. • 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

1. En la barra de menús, 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**, haga clic en **Configuración 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 UEM ni ninguno de sus componentes.
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 *<domain>**<username>*.

7. Repita los pasos del 4 al 6 para cada tipo de dispositivo.
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 crea más de un perfil de proxy, clasifique los perfiles según sea necesario. La clasificación que se especifique solo se aplicará si se asigna un perfil de proxy a los grupos de usuarios o de dispositivos. Seleccione un perfil y haga clic en ⇅ para moverlo hacia arriba o hacia abajo en la clasificación. Haga clic en **Guardar**.

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.

Si configura una red VPN por aplicación para BlackBerry Secure Connect Plus, para iOS y dispositivos de iPadOS, 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 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 activar BlackBerry Secure Connect Plus, siga los pasos siguientes:

Paso	Acción
1	Verifique que el dominio BlackBerry UEM de la empresa cumpla los requisitos para utilizar BlackBerry Secure Connect Plus.
2	Active BlackBerry Secure Connect Plus en el perfil de conectividad de la empresa predeterminado o en un perfil de conectividad de la empresa personalizado que haya creado.
3	De manera opcional, especifique la configuración DNS adecuada para la aplicación BlackBerry Connectivity.
4	Si tiene un entorno local que incluye dispositivos Android Enterprise y Samsung Knox Workspace con BlackBerry Dynamics, optimice las conexiones de túnel seguras.
5	Asigne el perfil de conectividad de empresa a cuentas de usuario y grupos.

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:

Entorno	Requisitos
Todos los entornos de UEM	• El firewall de la empresa debe permitir conexiones salientes a través del puerto 3101 a <*region*>.turnb.bbsecure.com y <*region*>.bbsecure.com. Si configura UEM para que utilice un servidor proxy, verifique que dicho servidor permita conexiones a estos subdominios a través del puerto 3101. • En cada instancia de 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 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.
UEM local	• Si su entorno 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. • Opcionalmente, puede instalar instancias adicionales de BlackBerry Secure Connect Plus instalando más de una BlackBerry Connectivity Node. • Opcionalmente, puede crear un grupo de servidores para dirigir el tráfico de BlackBerry Secure Connect Plus a una ruta regional específica a BlackBerry Infrastructure.
UEM Cloud	• Debe instalar BlackBerry Connectivity Node o actualizarlo a la versión más reciente. Al instalar o actualizar BlackBerry Connectivity Node, BlackBerry Secure Connect Plus también se instala o actualiza. Debe asegurarse de activar BlackBerry Connectivity Node antes de activar BlackBerry Secure Connect Plus. • Si enruta los datos que se transfieren entre BlackBerry Secure Connect Plus y BlackBerry Infrastructure a través de un servidor proxy TCP (Transparent o SOCKS v5), puede configurar los valores del proxy mediante la consola de administración de BlackBerry Connectivity Node (Configuración general > Proxy).

En los dispositivos compatibles:

Perfil	Descripción
iOS y iPadOS	• Los dispositivos se deben activar con BlackBerry UEM Client; para los dispositivos DEP de Apple, debe distribuir UEM Client a los usuarios desde UEM y, a continuación, indicar a los usuarios que abran UEM Client y completen el proceso de configuración • Tipo de activación de los controles 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	• Una versión compatible de Samsung Knox.
	• Cualquiera de los tipos de activación siguientes:
	  • Trabajo y personal: control total (Samsung Knox)
	  • Trabajo y personal: privacidad de usuario (Samsung Knox)

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).

Antes de empezar: Compruebe que el dominio de UEM de la empresa cumpla con los requisitos para usar BlackBerry Secure Connect Plus.

1. En la barra de menús de la consola de administración, haga clic en **Políticas y perfiles > Redes y conexiones > Conectividad de empresa**.
2. Edite un perfil de conectividad de empresa existente o cree uno nuevo.
3. 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.
4. Configure los valores correspondientes de la configuración de perfil de cada tipo de dispositivo. Para obtener más información acerca de cada configuración de perfil, consulte Configuración del perfil de conectividad de empresa.
5. Haga clic en **Agregar**.
6. Asigne el perfil a las cuentas de grupos o usuarios.

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 los dispositivos 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. Seleccione un perfil y haga clic en ↓↑ para moverlo hacia arriba o hacia abajo en la clasificación. Haga clic en **Guardar**.

- 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.
- Opcionalmente, especifique la configuración del DNS para la aplicación BlackBerry Connectivity.

Actualización de la aplicación BlackBerry Connectivity

La aplicación BlackBerry Connectivity más reciente está disponible en Google Play y en BlackBerry myAccount Software Downloads.

- **Usuarios de Android:** indique a los usuarios del dispositivo que actualicen a las versiones más recientes de BlackBerry UEM Client y de la aplicación BlackBerry Connectivity disponibles en Google Play. Para los dispositivos que no tienen acceso a Google Play, siga las instrucciones de Actualización de la aplicación BlackBerry Connectivity para los dispositivos Samsung Knox Workspace y Android Enterprise que no tienen acceso a Google Play.
- **Usuarios de Samsung Knox Workspace:**
  - Para los dispositivos Knox que tienen habilitada la gestión de aplicaciones Google Play, indique a los usuarios de los dispositivos que actualicen a las versiones más recientes de las aplicaciones BlackBerry UEM Client y BlackBerry Connectivity disponibles en Google Play. En la consola de administración de UEM, asegúrese de configurar la aplicación BlackBerry Connectivity que se debe enviar a "Todos los dispositivos Android" y asígnela a los usuarios y grupos adecuados.
  - En el caso de los dispositivos Knox que no tienen activada la administración de aplicaciones Google Play, siga las instrucciones de Actualización de la aplicación BlackBerry Connectivity para los dispositivos Samsung Knox Workspace y Android Enterprise que no tienen acceso a Google Play.

Nota: Si utiliza perfiles de certificado de CA para distribuir certificados de CA a dispositivos Android o Knox Workspace, compruebe que los certificados que ha cargado están codificados con DER con una extensión de archivo .der o codificados con PEM con una extensión de archivo .pem. Los certificados de CA que no cumplan estos requisitos pueden provocar problemas de conexión para la aplicación BlackBerry Connectivity.

Actualización de la aplicación BlackBerry Connectivity para los dispositivos Samsung Knox Workspace y Android Enterprise que no tienen acceso a Google Play

Siga las instrucciones que se indican a continuación para actualizar la aplicación BlackBerry Connectivity en los dispositivos de los usuarios a la versión más reciente.

Para beneficiarse de las últimas actualizaciones del servidor, se recomienda actualizar a la última versión de BlackBerry UEM.

Antes de empezar:

- Visite BlackBerry myAccount Software Downloads para descargar la versión más reciente de la aplicación BlackBerry Connectivity. Guarde los archivos en todos los equipos que alojen una instancia de UEM.
- Indique a los usuarios de dispositivos Knox Workspace que actualicen BlackBerry UEM Client a la versión más reciente disponible en Google Play.
- Para las activaciones Knox Workspace , dado que la versión más reciente de la aplicación BlackBerry Connectivity está disponible en Google Play, los usuarios pueden actualizar la aplicación por cuenta propia. Debe seguir igualmente estos pasos para configurar la compatibilidad de UEM con la aplicación.
- Para las activaciones Android Enterprise, los usuarios pueden actualizar a la versión más reciente de la aplicación BlackBerry Connectivity desde Google Play por su cuenta si Google Play está habilitado en el espacio de trabajo. Debe seguir igualmente estos pasos para configurar la compatibilidad de UEM con la aplicación.
- Para configurar UEM para que admita la aplicación BlackBerry Connectivity para dispositivos que requieren BlackBerry Secure Connect Plus:

1. En la consola de administración de UEM, haga clic en la opción **Aplicaciones** de la barra de menú.
2. Haga clic en > **Aplicaciones internas**.
3. Haga clic en **Examinar** y seleccione el archivo .apk de la aplicación BlackBerry Connectivity más reciente para Android.
4. Haga clic en **Agregar**.
5. En el campo **Enviar a**, seleccione **Todos los dispositivos Android**.
6. Anule la selección de **Publicar la aplicación en el dominio de Google**.
7. Haga clic en **Agregar**.
8. Asigne la aplicación que ha añadido en el paso anterior a los dispositivos Samsung Knox Workspace y Android Enterprise que no tengan acceso a Google Play. La disposición de la aplicación debe establecerse en **Obligatoria**.

Después de terminar: UEM envía una notificación de actualización de política a UEM Client en los dispositivos Knox Workspace. UEM Client actualiza la aplicación BlackBerry Connectivity cuando se asigna como aplicación obligatoria.

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.

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	Para especificar los dominios que están autorizados a iniciar una conexión VPN en Safari.
Dominios de calendario	Especifique el dominio que puede iniciar la conexión VPN en Calendario.
Dominios de contactos	Especifique los dominios que pueden iniciar la conexión VPN en Contactos.
Dominios de correo	Especifique los dominios que pueden iniciar la conexión VPN en Correo.
Dominios asociados	Especifique los dominios asociados.
Dominios excluidos	Especifique los dominios excluidos.
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.
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. 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 UEM Client se comunique con BlackBerry Infrastructure a través de UEM. Para obtener más información acerca de cómo abrir los puertos del firewall cuando las aplicaciones de trabajo utilizan BlackBerry Secure Connect Plus, consulte KB 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. Consulte Optimización de las conexiones de túnel seguras para dispositivos Android que utilizan aplicaciones de BlackBerry Dynamics. 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".
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".

Configuración	Descripción
Perfil de proxy	Puede seleccionar un perfil proxy que configuró para enrutar el tráfico de túnel seguro a través de un servidor proxy. Esta opción es compatible con dispositivos con los tipos de activación Android Enterprise. BlackBerry Secure Connect Plus admite tanto la configuración PAC como la configuración manual del servidor proxy en el perfil de proxy, pero tome nota de las limitaciones detalladas en setHttpProxy de developer.android.com. La compatibilidad con proxy web de BlackBerry Secure Connect Plus requiere la aplicación BlackBerry Connectivity versión 1.0.25.x o posterior o UEM Client 12.44.x o posterior.

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

Puede especificar los servidores DNS que desea que la aplicación BlackBerry Connectivity utilice en las conexiones de túnel seguro. 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.

1. Lleve a cabo una de las siguientes acciones:
   - En un entorno local, en la consola de administración de UEM, haga clic en **Configuración > Infraestructura > BlackBerry Secure Connect Plus** en la barra de menús.
   - En un entorno de nube, en el panel izquierdo de la consola de BlackBerry Connectivity Node (http:/localhost:8088), haga clic 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) Seleccione 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 menús de la consola de administración, haga clic en **Políticas y perfiles > Redes y conexiones > Conectividad de BlackBerry Dynamics**.
2. Edite el perfil asignado a los dispositivos Android Enterprise y Samsung Knox Workspace.

3. Desactive la casilla de verificación **Enrutar todo el tráfico**.
4. En la sección **Tipo de ruta de dominio permitida de forma predeterminada**, seleccione **Directa** para dirigir el tráfico directamente desde la aplicación al dominio sin pasar por BlackBerry Proxy.
5. 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.

BlackBerry Secure Connect Plus no se inicia

Causa posible

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

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** esté seleccionado 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 una nueva instalación de 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. Navegue hasta `<drive>:\Program Files\BlackBerry\UEMSecureConnectPlus\config\blackberry\` y ejecute **configureRRAS.bat**
5. Navegue hasta `<drive>:\Program Files\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

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 utilice 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.

Habilitación de la autenticación automática para dispositivos iOS

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.

Puede 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. Puede especificar los ajustes para una extensión personalizada o usar 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 de la consola de administración, haga clic en **Políticas y perfiles > Redes y conexiones > Extensión de registro único**.
2. Haga clic en +.
3. Escriba un nombre y una descripción para el perfil.
4. En la lista desplegable **Tipo de extensión de registro único**, haga clic en **Extensión personalizada** o **Extensión Kerberos integrada** 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.** Seleccione el tipo de inicio de sesión adecuado. **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 autodetección 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 preferidos**, haga clic en + para especificar los servidores preferidos si no se pueden detectar mediante DNS. Especifique cada servidor con el mismo formato que se usa 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 personalizada de dominio-territorio**, introduzca cualquier asignación personalizada necesaria de dominios a nombres de territorio en formato de carga, como, por ejemplo `<key>sample-realm1</key><array><string>org</string></array>`. **j.** En el campo **Pista de inicio de sesión**, especifique el texto para mostrar en la parte inferior de la ventana de inicio de sesión de Kerberos.

5. Haga clic en **Guardar**.

Especificación de servidores DNS para 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.

1. En la barra de menús de la consola de administración, haga clic en **Políticas y perfiles > Redes y conexiones > DNS**.
2. Haga clic en +.
3. Escriba un nombre y una descripción para el perfil.
4. Haga clic en la pestaña de un tipo de dispositivo.
5. Seleccione el protocolo DNS utilizado para comunicarse con el servidor DNS.
6. 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.

7. Para evitar que los usuarios desactiven la configuración, seleccione la casilla de verificación **No permitir al usuario desactivar la configuración de DNS**. Esta opción solo afecta a los dispositivos supervisados.
8. 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.
9. En el campo **Dominios**, especifique la lista de cadenas de dominio que se deban utilizar para determinar qué consultas DNS utilizarán los servidores DNS.
10. En el campo **Reglas de DNS a petición**, especifique las reglas de DNS a petición utilizando el formato de carga de ejemplo.
11. Repita los pasos del 5 al 10 para cada tipo de dispositivo.
12. Haga clic en **Guardar**.

Especificación del correo electrónico y 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 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.

1. En la barra de menús, haga clic en **Políticas y perfiles > Redes y conexiones > Dominios gestionados**.
2. Haga clic en +.
3. Escriba un nombre y una descripción para el perfil.
4. En el campo **Descripción**, escriba una descripción para el perfil.
5. En la sección **Dominios gestionados**, haga clic en +.
6. En el campo **Dominios de correo electrónico**, escriba un nombre de dominio de nivel superior (por ejemplo, `example.com` en lugar de `example.com/canada`).
7. Haga clic en **Agregar**.
8. 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.
9. En el campo **Dominios web**, escriba un nombre de dominio.
10. 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 con supervisados.
11. Haga clic en **Agregar**, a continuación, haga clic en **Agregar** de nuevo.

Después de terminar: Asigne los dominios gestionados a cuentas de usuario, grupos de usuarios o grupos de dispositivos.

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

Puede utilizar un perfil de uso de la red para controlar cómo utilizan la red móvil las aplicaciones en los dispositivos con 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.

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: Añada aplicaciones a la lista de aplicaciones y asígnelas a usuarios y grupos.

1. En la barra de menús de la consola de administración, haga clic en **Políticas y perfiles > Redes y conexiones > Uso de red**.
2. Haga clic en +.
3. Escriba un nombre y una descripción para el perfil.
4. Haga clic en +.
5. Lleve a cabo una de las siguientes acciones:
   - Haga clic en **Agregar una aplicación** y haga clic en una aplicación de la lista.
   - Seleccione la opción **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.***).
6. 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**.
7. 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**.
8. Haga clic en **Agregar**.
9. Repita los pasos 5 a 9 para cada aplicación que desee agregar a la lista.

Después de terminar: Si ha creado más de un perfil de uso de la red, clasifique los perfiles. Seleccione un perfil y haga clic en ↓↑ para moverlo hacia arriba o hacia abajo en la clasificación. Haga clic en **Guardar**.

Asigne el perfil de uso de la red a cuentas de usuario, grupos de usuarios o grupos de dispositivos.

Creación de un perfil de filtro de contenido web en dispositivos 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. 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).

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. 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.

1. En la barra de menús, haga clic en **Políticas y perfiles > Redes y conexiones > Filtro de contenido web**.
2. Haga clic en +.
3. Escriba un nombre y una descripción para el perfil de filtro de contenido web.
4. 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 **Marcadores de sitios web 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. Repita los pasos b y c para cada sitio web permitido.

Tarea	Pasos
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 + junto a **URL permitidas**. **2.** Escriba la dirección web para la que desea permitir el acceso. **3.** Repita según sea necesario para añadir sitios web adicionales. **c.** Opcionalmente, lleve a cabo las acciones siguientes: **1.** Haga clic en + junto a **URL en la lista negra**. **2.** Escriba la dirección web para la que desea denegar el acceso. **3.** Repita según sea necesario para añadir sitios web adicionales.

5. Haga clic en **Agregar**.

Después de terminar: Asigne el perfil del filtro de contenidos web a cuentas de usuario, grupos de usuarios o grupos de dispositivos.

Creación de un perfil de AirPrint para dispositivos iOS

Los perfiles de AirPrint pueden ayudar a los usuarios a encontrar impresoras que sean compatibles con AirPrint, a las que puedan 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 especifican el lugar en el que se encuentran los recursos. Puede configurar y asignar perfiles de AirPrint a los dispositivos con iOS y iPadOS para que los usuarios no tengan que configurar las impresoras manualmente.

1. En la barra de menús, haga clic en **Políticas y perfiles > Redes y conexiones > AirPrint**.
2. Haga clic en +.
3. Escriba un nombre y una descripción para el perfil.
4. En la sección **Configuración de AirPrint**, haga clic en +.
5. En el campo **Dirección IP**, escriba la dirección IP de la impresora o del servidor de AirPrint.
6. 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
7. Opcionalmente, si las conexiones de AirPrint están protegidas mediante TLS, seleccione la casilla de verificación **Forzar TLS**.
8. Opcionalmente, si el puerto difiere del predeterminado por el protocolo de impresión de Internet, escriba el número de puerto en el campo **Puerto**.
9. Haga clic en **Agregar**y, a continuación, haga clic en **Agregar** de nuevo.

Después de terminar: Asigne el perfil de AirPrint a cuentas de usuarios, grupos de usuarios o grupos de dispositivos.

Creación de un perfil de AirPlay para dispositivos iOS

AirPlay es una función de que permite mostrar fotos o transmitir música y vídeo a dispositivos AirPlay compatibles, como Apple TV, AirPort Express o altavoces con 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 aunque no sepan 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.

1. En la barra de menús, haga clic en **Políticas y perfiles > Redes y conexiones > AirPlay**.
2. Haga clic en +.
3. Escriba un nombre y una descripción para el perfil de AirPlay.
4. Haga clic en + en la sección **Dispositivos de destino permitidos**.
5. En el campo **Nombre del dispositivo**, escriba el nombre del dispositivo AirPlay para el que desea proporcionar la contraseña. Puede encontrar el nombre del dispositivo AirPlay en la configuración 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.
6. En el campo **Contraseña**, escriba la contraseña correcta.
7. Haga clic en **Agregar**.
8. Haga clic en + en la sección **Dispositivos de destino permitidos para los dispositivos supervisados**.
9. En el campo **ID del dispositivo**, escriba el ID del dispositivo AirPlay al que desea permitir que se conecten los dispositivos supervisados. Puede encontrar el ID del dispositivo AirPlay en los ajustes del dispositivo. Los dispositivos supervisados solo se podrán conectar a los dispositivos AirPlay de la lista.
10. Haga clic en **Agregar**.

Después de terminar: Asigne el perfil AirPlay a cuentas de usuarios, grupo de usuarios o grupo de dispositivos.

Creación de un perfil de nombre 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 para operadores a los dispositivos con Android de los usuarios. Los perfiles de nombre de punto de acceso son compatibles con los dispositivos con activaciones de Solo espacio de trabajo o 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 casilla de verificación "Forzar el dispositivo a usar la configuración del perfil de nombre de punto de acceso" en la regla de políticas de TI.

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

1. En la barra de menús, haga clic en **Políticas y perfiles > Redes y conexiones > Nombre de punto de acceso**.

2. Haga clic en +.
3. Escriba un nombre y una descripción para el perfil. Dicha información se muestra en los dispositivos.
4. En el campo **Nombre de punto de acceso**, escriba el nombre del punto de acceso.
5. 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.
6. Haga clic en **Guardar**.

Después de terminar: Asigne el perfil de nombre de punto de acceso a cuentas de usuarios, grupos de usuarios o grupos de dispositivos.

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.
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.
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.
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.
Contraseña	Si la configuración "Tipo de autenticación" se establece en un valor distinto de NINGUNO, especifique una contraseña si es necesario para la autenticación.

Configuración del perfil de nombre de punto de acceso	Descripción
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.
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.
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.

Uso de certificados de PKI con dispositivos o aplicaciones

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

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

- Realizar la autenticación mediante SSL/TLS cuando se conecte a servidores web que admitan TLS mutuo, incluido un servidor de correo de trabajo.
- Realizar la autenticación en una VPN o red Wi-Fi de trabajo.
- Cifrar y firmar mensajes de correo electrónico mediante protección S/MIME.

Varios de los certificados utilizados con distintos fines se pueden guardar en un dispositivo. BlackBerry UEM proporciona una serie de perfiles para ayudar a administrar los certificados de PKI en el dispositivo. Por ejemplo:

- La confianza del servidor de CA puede asignarse a dispositivos y aplicaciones utilizando un perfil de certificado de CA.
- La inscripción automática de certificados puede asignarse a dispositivos y aplicaciones utilizando perfiles SCEP y de credenciales de usuario.
- La recuperación de certificados de cifrado público puede asignarse a dispositivos y aplicaciones utilizando el perfil de recuperación de certificados.
- La comprobación del estado de revocación de certificados puede asignarse a dispositivos y aplicaciones utilizando perfiles CRL y OCSP.

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

Paso	Acción
1	Si es necesario, integre BlackBerry UEM al software de PKI de su empresa.
2	Cree uno o más perfiles de certificados de CA para enviarlos a los dispositivos y las aplicaciones.
3	Cree perfiles SCEP, perfiles de credenciales de usuario o perfiles de certificado compartido, o cargue certificados para un usuario específico para enviar certificados de cliente a los dispositivos y las aplicaciones.
4	Si es necesario, asocie perfiles de certificado con perfiles de Wi-Fi, VPN o correo electrónico.
5	Si es necesario, asigne los perfiles de certificado a las cuentas de usuario, a los grupos de usuarios o a los grupos de dispositivos.

Paso	Acción
6	Si utiliza certificados con una aplicación de BlackBerry Dynamics, en la configuración de la aplicación seleccione "Permitir que las aplicaciones de BlackBerry Dynamics utilicen certificados de usuario, perfiles SCEP y perfiles de credenciales de usuario".

Integración de BlackBerry UEM con el software PKI de la empresa

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

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

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

Conexión de BlackBerry UEM al software de Entrust de la empresa

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

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

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

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

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

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

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

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

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

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

Después de terminar:

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

Conexión de BlackBerry UEM al software de OpenTrust de la empresa

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

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

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

Después de terminar:

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

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

Conexión de BlackBerry UEM a un conector PKI de BlackBerry Dynamics

Si desea utilizar el software PKI de su empresa para la inscripción de certificados para las aplicaciones BlackBerry Dynamics y su software PKI no es compatible con una conexión directa con BlackBerry UEM, puede configurar un conector PKI de BlackBerry Dynamics para comunicarse con su CA y vincular UEM con el conector PKI. En entornos BlackBerry UEM Cloud, debe tener instalado BlackBerry Connectivity Node para permitir la comunicación de UEM con el conector PKI a través de BlackBerry Cloud Connector.

Para obtener más información sobre la configuración de un conector de PKI de BlackBerry Dynamics, consulte la documentación del Protocolo de administración de certificados de usuario y conector de PKI.

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

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

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

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

Las soluciones PKI basadas en aplicaciones, como Purebred, incluyen una aplicación instalada en un dispositivo que se comunica con una CA para inscribir certificados y añadirlos al dispositivo. Puede utilizar una solución

PKI basada en aplicaciones para proporcionar certificados para que lo utilicen las aplicaciones de BlackBerry Dynamics.

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

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

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

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

Después de terminar: Efectúe una de las acciones siguientes:

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

Integración de certificados de cliente en dispositivos y aplicaciones

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

Cómo se agrega el certificado	Descripción	Dispositivos compatibles
Durante la activación del dispositivo	BlackBerry UEM envía los certificados a los dispositivos durante el proceso de activación. Los dispositivos utilizan estos certificados para establecer conexiones seguras entre el dispositivo y UEM.	Todas
Perfiles SCEP	Puede crear perfiles SCEP que los dispositivos pueden utilizar para conectarse y obtener certificados de cliente de la CA de su empresa mediante un servicio SCEP. Los dispositivos y aplicaciones BlackBerry Dynamics pueden utilizar estos certificados para realizar la autenticación basada en certificados y para conectarse a la red Wi-Fi, la VPN y el servidor de correo del trabajo.	iOS macOS Android Windows 10

Cómo se agrega el certificado	Descripción	Dispositivos compatibles
Conexión a la solución de PKI de la empresa	Si su empresa utiliza una solución de PKI, como los productos de software de Entrust o OpenTrust para emitir y gestionar certificados, puede crear perfiles de credenciales de usuario que los dispositivos pueden utilizar para obtener certificados de cliente de la CA de su empresa. Los dispositivos con BlackBerry Dynamics utilizan estos certificados para la autenticación basada en certificados de las aplicaciones de BlackBerry Dynamics. Otros dispositivos utilizan estos certificados para realizar la autenticación basada en certificados desde el navegador y para conectarse a la red Wi-Fi, la VPN y el servidor de correo del trabajo.	iOS (macOS solo para BlackBerry Access) Android (Windows 10 solo para BlackBerry Access)
Perfiles de certificado compartido	Los perfiles de certificado compartido especifican el certificado de cliente que UEM envía a los dispositivos iOS, macOS y Android. UEM envía el mismo certificado de cliente a todos los usuarios a los que se ha asignado el perfil. El administrador debe tener acceso al certificado y la clave privada para crear un perfil de certificado compartido.	iOS macOS Android
Envío de certificados de cliente a cuentas de usuario individuales	Puede agregar un certificado de cliente a una cuenta de usuario. UEM puede enviar el certificado a los dispositivos iOS y Android del usuario. Si el certificado se asocia con un perfil de credenciales de usuario, los dispositivos pueden utilizar estos certificados para conectarse a su red Wi-Fi de trabajo, VPN de trabajo y servidor de correo de trabajo. El administrador debe tener acceso al certificado y la clave privada para enviar el certificado del cliente al usuario.	iOS Android
Carga de usuarios en UEM Self-Service	Los usuarios pueden cargar certificados en BlackBerry UEM Self-Service. A continuación, UEM inserta el certificado en los dispositivos de los usuarios. Si el certificado se asocia con un perfil de credenciales de usuario, los dispositivos y las aplicaciones BlackBerry Dynamics pueden utilizar estos certificados para una autenticación basada en certificados y para conectarse a su red Wi-Fi de trabajo, VPN de trabajo y servidor de correo de trabajo.	iOS Android
Importación por parte de los usuarios	Los usuarios pueden añadir certificados al almacén de claves nativo del dispositivo para usarlos con las aplicaciones BlackBerry Dynamics.	Android

Envío de certificados a dispositivos y aplicaciones mediante perfiles

Puede enviar certificados a dispositivos y aplicaciones mediante los siguientes perfiles:

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

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

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

Para que las aplicaciones de BlackBerry Dynamics utilicen certificados enviados por perfiles, debe seleccionar "Permitir que las aplicaciones de BlackBerry Dynamics utilicen certificados de usuario, perfiles SCEP y perfiles de credenciales de usuario" para la aplicación específica en la pantalla **Aplicación**, en la pestaña **Configuración > BlackBerry Dynamics**.

El tipo de perfil que seleccione dependerá de cómo su empresa utilice los certificados y los tipos de dispositivos que admita la empresa. Considere las siguientes directrices:

- Para utilizar perfiles SCEP, debe tener una CA que admita SCEP.
- Si ha configurado una conexión entre UEM y la solución PKI de la empresa, utilice los perfiles de credenciales de usuario para enviar certificados a los dispositivos. Puede conectarse directamente a una CA de Entrust o

CA de OpenTrust. También puede utilizar un conector de PKI de BlackBerry Dynamics para conectarse a un servidor CA a fin de inscribir certificados para dispositivos con BlackBerry Dynamics.

- Para utilizar certificados con aplicaciones de BlackBerry Dynamics, debe utilizar un perfil de credenciales de usuario o agregar certificados a cuentas de usuario individuales.
- Para permitir que los usuarios carguen certificados que puedan utilizar para conectarse a su red Wi-Fi de trabajo, red VPN de trabajo y servidor de correo del trabajo, utilice un perfil de credenciales de usuario.
- Para utilizar certificados de cliente para Wi-Fi, VPN y autenticación del servidor de correo, debe asociar el perfil de certificado con un perfil Wi-Fi, VPN o de correo electrónico.
- Los dispositivos Android Enterprise no son compatibles con el uso de los certificados que UEM ha enviado a los dispositivos para la autenticación Wi-Fi.
- Los perfiles de certificado compartido y los perfiles que agrega a las cuentas de usuario no mantienen la clave privada en privado porque se debe tener acceso a ella. La conexión a un CA mediante perfiles de credenciales de usuario o SCEP es más segura porque la clave privada solo se envía al dispositivo para el que se emitió el certificado.

Envío de certificados de CA a dispositivos y aplicaciones

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

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

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

Creación de un perfil de certificado de CA

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

1. En la barra de menús de la consola de administración, haga clic en **Políticas y perfiles > Certificados > Certificado de CA**.
2. Haga clic en +.
3. Escriba un nombre y una descripción para el perfil. Cada perfil de certificado de CA debe tener un nombre único. Algunos nombres (por ejemplo, ca_1) están reservados.
4. En el campo **Archivo de certificado**, haga clic en **Examinar** para ubicar el archivo de certificado.
5. Si el certificado CA se envía a los dispositivos macOS, en la pestaña macOS, en la lista desplegable **Aplicar perfil a**, seleccione **Usuario** o **Dispositivo**.
6. Haga clic en **Agregar**.

Después de terminar: Asigne el certificado de CA a cuentas de usuarios, grupos de usuarios o grupos de dispositivos.

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

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

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

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

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

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

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

1. En la barra de menús, haga clic en **Políticas y perfiles > Certificados > Credenciales de usuario**.
2. Haga clic en +.
3. Escriba un nombre y una descripción para el perfil. Cada perfil de certificado debe tener un nombre único.
4. En la lista desplegable **Conexión con la autoridad de certificación**, seleccione **Certificado cargado manualmente**.
5. Si administra dispositivos Android Enterprise y desea evitar que los usuarios seleccionen el certificado para utilizarlo con otros fines, en la pestaña **Android**, seleccione la casilla de verificación **Ocultar certificado en dispositivos Android Enterprise**.
6. Haga clic en **Agregar**.

Después de terminar:

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

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

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

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

Antes de empezar:

- Configure una conexión al software de Entrust o OpenTrust de su empresa.
- Contacte con el administrador de Entrust o de OpenTrust de la empresa para confirmar qué perfil de PKI debe seleccionar.
- Solicite al administrador de Entrust o OpenTrust los valores para el perfil que debe proporcionar.

- Si el sistema OpenTrust de su empresa está configurado para devolver solo claves bajo custodia, el administrador de OpenTrust debe verificar que haya certificados para cada usuario en el sistema OpenTrust. Al asignar un perfil de credenciales de usuario a los usuarios en UEM no se crean automáticamente certificados para usuarios en OpenTrust. En este caso, un perfil de credenciales de usuario solo puede distribuir certificados a los usuarios que tienen un certificado existente en el sistema OpenTrust.

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

      Si se establece el tipo de SAN en "Nombre de RFC822", el valor debe ser una dirección de correo válida. Si se establece en "URI", el valor debe ser una URL válida que incluya el protocolo y la dirección IP o FQDN. Si se establece en "Nombre principal de NT", el valor debe ser un nombre principal válido. Si se establece en "Nombre de DNS", el valor debe ser un FQDN válido.
8. Especifique el **Período de renovación** del certificado. El periodo puede ser entre 1 y 120 días.
9. Haga clic en **Agregar**.

Después de terminar:

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

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

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

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

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

Antes de empezar:

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

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

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

   Si no se selecciona esta opción, solo las aplicaciones de BlackBerry Dynamics pueden utilizar la credencial inteligente.
7. Si la credencial inteligente se va a enviar a aplicaciones de BlackBerry Dynamics, haga lo siguiente en la pestaña **BlackBerry Dynamics**:
   a) Si desea permitir que los usuarios descarten la inscripción de certificados y la completen más adelante, seleccione **Permitir inscripción de certificados opcional**. La inscripción de certificados opcional es compatible con dispositivos con iOS y Android para los siguientes tipos de perfiles de credenciales de usuario: proveedor basado en dispositivos (aplicación), credencial inteligente de confianza y almacén de claves nativo.
   b) Si desea que el dispositivo elimine credenciales duplicadas, seleccione **Eliminar certificados duplicados**. El dispositivo elimina la credencial que tiene la fecha de inicio más inmediata.
   c) Si desea que el dispositivo elimine credenciales caducadas, seleccione **Eliminar certificados caducados**.
   d) Para permitir que todas las aplicaciones de BlackBerry Dynamics utilicen las credenciales inteligentes, seleccione **Permitir que todas las aplicaciones utilicen certificados**.
   e) Para especificar las aplicaciones de BlackBerry Dynamics que utilizan las credenciales inteligentes, seleccione **Permitir que aplicaciones específicas utilicen certificados** ya haga clic en + para especificar las aplicaciones. Debe incluir BlackBerry UEM Client en la lista de aplicaciones.
8. Haga clic en **Agregar**.

Después de terminar:

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

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

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

- Para permitir que las aplicaciones de BlackBerry Dynamics utilicen un certificado del almacén de claves nativo en dispositivos con Android.
- Para permitir que las aplicaciones de BlackBerry Dynamics utilicen un certificado del almacén de claves nativo para acceder a tokens criptográficos desde aplicaciones PKI en dispositivos con iOS.

- Para permitir que la aplicación de BlackBerry Access utilice un certificado del almacén de claves nativo en dispositivos con macOS o Windows 10.

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

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

1. En la barra de menús, haga clic en **Políticas y perfiles > Certificados > Credenciales de usuario**.
2. Haga clic en +.
3. Escriba un nombre y una descripción para el perfil. Cada perfil de certificado debe tener un nombre único.
4. En la lista desplegable **Conexión con la autoridad de certificación**, seleccione **Almacén de claves nativo**.
5. En la sección **Plataformas compatibles**, seleccione los tipos de SO del dispositivo que desea que este perfil admita.
6. En la sección **Inscripción de certificados**, seleccione la casilla de verificación **Permitir inscripción de certificados opcional** si desea permitir que los usuarios de Android descarten la inscripción de certificados y la completen más tarde.
7. Para especificar qué certificado utilizará la aplicación de BlackBerry Dynamics, realice las acciones siguientes:
   a) Junto a **Emisores**, haga clic en + y escriba el nombre del emisor.

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

      ```
      CN=Acme_cert SMIME,OU=Acme_Legal,O=Acme,C=Can
                                CN=Acme_cert SMIME,OU=Acme_Legal,O=Acme
                                CN=Acme_cert TLS
      ```

   b) En la sección **Uso de la clave**, seleccione las operaciones con las que es compatible el certificado.

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

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

Después de terminar:

- Para permitir que las aplicaciones BlackBerry Dynamics utilicen certificados, haga clic en **Aplicaciones** en la barra de menús. Haga clic en la aplicación de BlackBerry Dynamics que desea cambiar y, a continuación, en la pestaña **Configuración > BlackBerry Dynamics**, seleccione la casilla de verificación **Permitir que las aplicaciones de BlackBerry Dynamics utilicen perfiles SCEP de certificados de usuario y perfiles de credenciales de usuario**.
- Asigne el perfil a las cuentas de usuario y los grupos de usuarios.

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

1. En la barra de menús, haga clic en **Políticas y perfiles > Certificados > Credenciales de usuario**.
2. Haga clic en +.
3. Escriba un nombre y una descripción para el perfil.
4. En la lista desplegable **Conexión con la autoridad de certificación**, haga clic en la conexión de PKI de BlackBerry Dynamics que ha configurado.
5. Si el usuario debe proporcionar una contraseña para solicitar un certificado, seleccione **Requerir contraseña introducida por el usuario u OTP**.
6. Si desea permitir que el dispositivo solicite automáticamente un nuevo certificado antes de que el certificado actual caduque, seleccione **Activar la renovación de certificados** y especifique el número de días previos a la caducidad en que los dispositivos deben solicitar un nuevo certificado.
7. Si desea que el dispositivo elimine los certificados caducados, seleccione la casilla de verificación **Eliminar certificados caducados**.
8. Si desea que el dispositivo elimine los certificados duplicados, seleccione la casilla de verificación **Eliminar certificados duplicados**.
9. Haga clic en **Agregar**.

Después de terminar:

- Para permitir que las aplicaciones BlackBerry Dynamics utilicen certificados, haga clic en **Aplicaciones** en la barra de menús. Haga clic en la aplicación de BlackBerry Dynamics que desea cambiar y, a continuación, en la pestaña **Configuración > BlackBerry Dynamics**, seleccione la casilla de verificación **Permitir que las aplicaciones de BlackBerry Dynamics utilicen perfiles SCEP de certificados de usuario y perfiles de credenciales de usuario**.
- Asigne el perfil a las cuentas de usuario y los grupos de usuarios.
- Si actualiza el conector PKI, haga clic en **Actualizar capacidades de PKI** para actualizar las funciones PKI admitidas para el perfil.
- Si desea renovar los certificados inscritos a través del conector PKI, haga clic en **Actualizar capacidades de PKI > Renovar** para ordenar a todos los dispositivos habilitados para BlackBerry Dynamics que tengan asignado el perfil que soliciten la renovación del certificado.

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

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

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

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

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

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

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

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

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

Antes de empezar: Configuración de BlackBerry UEM Client para que sea compatible con certificados basados en aplicación.

1. En la consola de administración de UEM, haga clic en la opción **Aplicaciones** de la barra de menú.
2. En la lista de aplicaciones, seleccione BlackBerry UEM Client.
3. En la sección **Configuración de aplicación**, haga clic en + .

4. En el campo **Nombre de aplicación**, escriba un nombre para la aplicación.
5. En el campo **UTI schemes**, especifique los esquemas de UTI de la solución PKI basada en aplicación de su empresa. Por ejemplo, si utiliza la aplicación Purebred, use los esquemas siguientes: `purebred.select.all-user`, `purebred.select.no-filter`, `purebred.zip.all-user`, `purebred.zip.no-filter`.
6. Haga clic en **Guardar**.

Después de terminar: Asigne UEM Client con la configuración de aplicación que ha creado a los usuarios y dispositivos que desea que utilicen la solución PKI basada en aplicaciones.

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

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

Antes de empezar: Asegúrese de que ha realizado una de las siguientes acciones:

- Si su entorno utiliza una solución de PKI basada en aplicaciones con dispositivos iOS, conecte BlackBerry UEM a la solución de PKI basada en aplicaciones de su empresa.
- Si su entorno utiliza una solución de PKI basada en aplicaciones con dispositivos iOS y la aplicación de PKI no es una aplicación BlackBerry Dynamics, configure BlackBerry UEM Client para que admita certificados basados en aplicaciones.

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

Tarea	Pasos
Configurar BlackBerry Work cuando su empresa utiliza BEMS	**a.** En la pestaña **Configuración básica**, en la sección **Configuración de seguridad**, seleccione la casilla de verificación **Usar certificado de cliente en lugar de inicio de sesión/contraseña**. **b.** Para activar la autodetección del servidor de Microsoft Exchange en el que se encuentran los usuarios, en la sección **Configuración del cliente**, seleccione la casilla de verificación **Utilizar BEMS para realizar la detección automática del punto final EAS/EWS para el usuario**. **c.** En la pestaña **Configuración avanzada**, en la sección **Configuración del certificado TLS**, escriba el nombre del perfil de credenciales de usuario para el dispositivo.

Tarea	Pasos
Configurar BlackBerry Work cuando su empresa no utiliza BEMS	**a.** Haga clic en la pestaña **Configuración básica**. **b.** Si su servidor utiliza el formato de nombre de dominio\inicio de sesión del usuario, en la sección **Configuración de Exchange ActiveSync**, en el campo **Dominio predeterminado**, especifique el dominio de Windows NT predeterminado al que se conecta BlackBerry Work cuando los usuarios inician sesión. **c.** En el campo **Active Sync Server**, especifique el servidor de Exchange ActiveSync predeterminado al que BlackBerry Work se conecta cuando los usuarios inician sesión en BlackBerry Work (por ejemplo, cas.mydomain.com). **d.** En el campo **URL de detección automática**, especifique la URL de autodetección, si la sabe. Esto acelera el proceso de configuración de autodetección (por ejemplo, https://autodiscover.mydomain.com). **e.** En el campo **Tiempo de espera de conexión de autodetección en segundos (solo iOS)**, especifique el tiempo de espera de conexión de autodetección en segundos. **f.** En la sección **Configuración del certificado TLS**, en el campo **Nombre del perfil de credenciales de usuario**, escriba el nombre del perfil de credenciales de usuario.

5. Haga clic en **Guardar**.

Después de terminar: Cree una solución PKI basada en aplicaciones para utilizarla con los siguientes dispositivos:

- Dispositivos iOS: crear un perfil de credenciales de usuario para usar certificados basados en aplicaciones.
- Dispositivos Android: crear un perfil de credenciales de usuario para utilizar certificados del almacén de claves nativo.

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

Antes de empezar:

- Configuración de BlackBerry UEM Client para que sea compatible con certificados basados en aplicación.
- Asegúrese de que la aplicación PKI (por ejemplo, Purebred) esté instalada en los dispositivos de los usuarios.

1. En la barra de menús, haga clic en **Políticas y perfiles > Certificados > Credenciales de usuario**.
2. Haga clic en +.
3. Escriba un nombre y una descripción para el perfil.
4. En la lista desplegable **Conexión con la autoridad de certificación**, haga clic en el nombre de la aplicación que especificó al conectar BlackBerry UEM a su solución PKI. Si utiliza Purebred, seleccione BlackBerry UEM Client.
5. Para especificar qué certificado utilizará la aplicación de BlackBerry Dynamics, realice las acciones siguientes:
   a) En la sección **Uso de la clave**, seleccione las operaciones con las que es compatible el certificado.

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

Las aplicaciones de BlackBerry Dynamics solo utilizarán certificados si todos los valores de uso de la clave ampliados seleccionados están presentes en el certificado. Los certificados pueden tener más valores de uso de la clave ampliados.

c) Si el certificado se emitió para fines distintos al uso en correo electrónico, la autenticación de cliente y el inicio de sesión con tarjeta inteligente, seleccione **Uso de ID de objeto adicional**, haga clic en + y especifique el OID del uso de la clave. Por ejemplo, si el certificado se va a utilizar para autenticación de servidor, puede tener el OID 1.3.6.1.5.5.7.3.1.

d) Junto a **Emisores**, haga clic en + y escriba el nombre del emisor.

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

```
CN=Acme_cert SMIME,OU=Acme_Legal,O=Acme,C=Can
                                    CN=Acme_cert SMIME,OU=Acme_Legal,O=Acme
                                    CN=Acme_cert TLS
```

6. Si desea que el dispositivo elimine certificados caducados, seleccione **Eliminar certificados caducados**.
7. Si desea que el dispositivo elimine certificados duplicados, seleccione **Eliminar certificado duplicado**.
8. Haga clic en **Agregar**.

Después de terminar:

- Para permitir que las aplicaciones BlackBerry Dynamics utilicen certificados, haga clic en **Aplicaciones** en la barra de menús. Haga clic en la aplicación de BlackBerry Dynamics que desea cambiar y, a continuación, en la pestaña **Configuración > BlackBerry Dynamics**, seleccione la casilla de verificación **Permitir que las aplicaciones de BlackBerry Dynamics utilicen certificados de usuario, perfiles SCEP y perfiles de credenciales de usuario**.
- Asigne el perfil a las cuentas de usuario y los grupos de usuarios.

Envío de certificados de cliente a dispositivos y aplicaciones mediante SCEP

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

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

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

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

Crear un perfil SCEP

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

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

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

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

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

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

Común: ajustes del perfil SCEP

Común: configuración del perfil SCEP	Descripción
Conexión con la autoridad de certificación	Esta configuración especifica si la CA es Entrust, OpenTrust u otra CA.

Común: configuración del perfil SCEP	Descripción
URL	Este ajuste especifica la URL del servicio SCEP. La URL debe incluir el protocolo, el FQDN, el número de puerto y la ruta SCEP (la ruta CGI que se define en la especificación SCEP). Debe establecer un valor la configuración para activar un dispositivo correctamente. Las URL HTTPS de SCEP son compatibles con los dispositivos iOS.
Nombre de la instancia	Este ajuste especifica el nombre de la instancia de la autoridad de certificación. El valor puede ser cualquier cadena que sea entendida por el servicio SCEP. Por ejemplo, podría tratarse de un nombre de dominio como example.org. Si una CA tiene varios certificados de CA, este campo puede utilizarse para distinguir cuál se necesita.
Comprobar cadena de confianza de conexión al servidor SCEP	Esta configuración especifica si BlackBerry UEM verifica que la raíz CA del servidor SCEP se ha almacenado en el almacén de certificados UEM para permitir que UEM confíe en el servidor SCEP cuando se prueben las conexiones, se recuperen contraseñas de comprobación y actúe como proxy para las solicitudes de SCEP de los dispositivos.
Tipo de desafío SCEP	En la configuración se especifica si la contraseña de comprobación SCEP se genera dinámicamente o como una contraseña estática. Si la configuración se establece en "Estático", todos los dispositivos utilizarán la misma contraseña de comprobación. Para los dispositivos Windows, únicamente se admiten contraseñas "estáticas".
URL de generación de contraseñas de comprobación	En la configuración se especifica la URL que el dispositivo utiliza para obtener una contraseña de comprobación generada dinámicamente desde el servicio SCEP. La URL debe incluir el protocolo, el dominio, el puerto y la ruta SCEP (la ruta CGI que se define en la especificación SCEP). Esta configuración es válida únicamente si la opción "Tipo de desafío SCEP" se establece en "Dinámico".
Tipo de autenticación	En la configuración se especifica el tipo de autenticación que los dispositivos utilizan para conectarse al servicio SCEP y obtener una contraseña de comprobación. Esta configuración es válida únicamente si la opción "Tipo de desafío SCEP" se establece en "Dinámico".
Dominio	En la configuración se especifica el dominio utilizado para la autenticación NTLM cuando los dispositivos se conectan al servicio SCEP para obtener una contraseña de comprobación. Esta configuración es válida únicamente si la opción "Tipo de autenticación" se establece en "NTLM".

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

iOS: configuración del perfil de SCEP

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

iOS: configuración del perfil SCEP	Descripción
Tipo de SAN	Esta configuración especifica el tipo de nombre alternativo del asunto del certificado, si es necesario.
Valor de SAN	Esta configuración especifica la representación alternativa del asunto del certificado. El valor debe ser una dirección de correo, el nombre DNS del servidor CA, la URL completa del servidor. El ajuste "Tipo de SAN" determina el valor adecuado que se debe especificar. Si se establece en "Nombre de RFC822" el valor debe ser una dirección de correo válida. Si se establece en "URI", el valor debe ser una URL válida que incluya el protocolo y la dirección IP o FQDN. Si se establece en "Nombre principal de NT", el valor debe ser un nombre principal válido. Si se establece en "Nombre de DNS", el valor debe ser un FQDN válido.
Nombre principal de NT	Esta configuración especifica el nombre principal de NT para la generación del certificado. Esta configuración es válida únicamente si la opción "Tipo de SAN" se establece en un valor distinto de "Ninguno".
Caducidad del perfil	Especifique el número de días después de la emisión del certificado en el que el dispositivo solicita un nuevo certificado de la CA. El valor debe ser inferior al periodo de validez del certificado definido por la CA.

macOS: configuración del perfil de SCEP

macOS: configuración del perfil SCEP	Descripción
Usar BlackBerry UEM como proxy para solicitudes SCEP	En la configuración se especifica si todas las solicitudes SCEP desde los dispositivos se envían a través de BlackBerry UEM. Si la CA está detrás del firewall, la configuración permitirá inscribir certificados de cliente en los dispositivos sin exponer la CA fuera del firewall.
Utilice BlackBerry Connectivity Node para la conectividad CA	Esta configuración especifica si las solicitudes SCEP deben enrutarse a través de BlackBerry Connectivity Node. Esta configuración solo se muestra en BlackBerry UEM Cloud.
Aplicar perfil a	En la configuración se especifica si el perfil SCEP se aplica a la cuenta de usuario o al dispositivo.
Asunto	Esta configuración especifica el asunto del certificado, si es necesario para la configuración SCEP de la empresa. Escriba el asunto con el formato "/CN=<*common_name*>/O=<*domain_name*>". Si el perfil es para varios usuarios, puede utilizar una variable, como, por ejemplo: %UserDistinguishedName%.
Reintentos	En la configuración se especifica cuántas veces debe volver a intentarse la conexión al servicio SCEP si el intento de conexión falla.

macOS: configuración del perfil SCEP	Descripción
Intervalo entre reintentos	En la configuración se especifica el tiempo en segundos que hay que esperar antes de intentar conectarse al servicio SCEP.
Tamaño de clave	Esta configuración especifica el tamaño de clave para el certificado.
Huella dactilar	Esta configuración especifica la huella digital para inscribir un certificado SCEP. Si la CA utiliza HTTP en lugar de HTTPS, los dispositivos utilizan la huella digital para confirmar la identidad de la CA durante el proceso de inscripción. La huella dactilar no puede contener espacios.
Tipo de SAN	Esta configuración especifica el tipo de nombre alternativo del asunto del certificado, si es necesario.
Valor de SAN	Esta configuración especifica la representación alternativa del asunto del certificado. El valor debe ser una dirección de correo, el nombre DNS del servidor CA, la URL completa del servidor. El ajuste "Tipo de SAN" determina el valor adecuado que se debe especificar. Si se establece en "Nombre de RFC822" el valor debe ser una dirección de correo válida. Si se establece en "URI", el valor debe ser una URL válida que incluya el protocolo y la dirección IP o FQDN. Si se establece en "Nombre principal de NT", el valor debe ser un nombre principal válido. Si se establece en "Nombre de DNS", el valor debe ser un FQDN válido.
Nombre principal de NT	Esta configuración especifica el nombre principal de NT para la generación del certificado. Esta configuración es válida únicamente si la opción "Tipo de SAN" se establece en un valor distinto de "Ninguno".

Android: configuración del perfil de SCEP

En el caso de los dispositivos con tipos de activación de Android Management, consulte las Consideraciones sobre los tipos de activación de Android Management .

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

Android: configuración del perfil SCEP	Descripción
Algoritmo de cifrado	Esta configuración especifica el algoritmo de cifrado que los dispositivos con Android utilizan para la solicitud de inscripción de certificados.
Función hash	Esta configuración especifica la función hash que los dispositivos con Android utilizan para la solicitud de inscripción de certificados.
Huella digital de certificado	Esta configuración especifica el hash de cifrado hexadecimal del certificado raíz para la autoridad de certificación. Puede utilizar los siguientes algoritmos para especificar la huella digital: SHA-1, SHA-224, SHA-256, SHA-384 y SHA-512. Debe establecer un valor para esta configuración para que se activen correctamente dispositivos con Android Enterprise o Samsung Knox.
Renovación automática	Esta configuración especifica cuántos días antes de que caduque el certificado debe realizarse la renovación automática.
Perfiles de trabajo de Android y Samsung KNOX	
Asunto	Esta configuración especifica el asunto del certificado, si es necesario para la configuración SCEP de la empresa. Escriba el asunto en el formato "/CN=<*common_name*>/O=<*domain_name*>". Si el perfil es para varios usuarios, puede utilizar una variable como, por ejemplo: %UserDistinguishedName%.
Tipo de SAN	Esta configuración especifica el tipo de nombre alternativo del asunto del certificado, si es necesario.
Valor de SAN	Esta configuración especifica la representación alternativa del asunto del certificado. El valor debe ser una dirección de correo, el nombre DNS del servidor CA, la URL completa del servidor o el nombre principal. El ajuste "Tipo de SAN" determina el valor adecuado que se debe especificar. Si se establece en "Nombre de RFC822" el valor debe ser una dirección de correo válida. Si se establece en "URI", el valor debe ser una URL válida que incluya el protocolo y la dirección IP o FQDN. Si se establece en "Nombre principal de NT", el valor debe ser un nombre principal válido. Si se establece en "Nombre de DNS", el valor debe ser un FQDN válido.
Algoritmo de clave	Esta configuración especifica el algoritmo que los dispositivos utilizan para generar el par de claves del cliente. Debe seleccionar un algoritmo que sea compatible con su CA.
Intensidad de RSA	Esta configuración especifica la intensidad de RSA que los dispositivos utilizan para generar el par de claves del cliente. Debe introducir una intensidad de la clave que sea compatible con su CA. Esta configuración solo es válida si la opción "Algoritmo de clave" se establece en "RSA".
Uso de la clave	Esta configuración especifica las operaciones criptográficas que se pueden realizar con la clave pública que está incluida en el certificado.

Android: configuración del perfil SCEP	Descripción
Uso extendido de la clave	Esta configuración especifica la finalidad de la clave que está incluida en el certificado.

Windows 10: configuración del perfil de SCEP

Windows 10: configuración del perfil SCEP	Descripción
Almacén de certificados del usuario	Esta configuración especifica si el certificado debe almacenarse en la ubicación de certificados del usuario en el dispositivo.
Asunto	Esta configuración especifica el asunto del certificado, si es necesario para la configuración SCEP de la empresa. Escriba el asunto en el formato "/CN=<*common_name*>/O=<*domain_name*>". Si el perfil es para varios usuarios, puede utilizar una variable como, por ejemplo: %UserDistinguishedName%.
Tipo de SAN	Esta configuración especifica el tipo de nombre alternativo del asunto del certificado, si es necesario.
Valor de SAN	Esta configuración especifica la representación alternativa del asunto del certificado. El valor debe ser una dirección de correo, el nombre DNS del servidor CA, la URL completa del servidor. El valor apropiado para este ajuste dependerá del valor seleccionado para el ajuste "Tipo de SAN".
Reintentos	En la configuración se especifica cuántas veces debe volver a intentarse la conexión al servicio SCEP si el intento de conexión falla.
Intervalo entre reintentos	En la configuración se especifica el tiempo en segundos que hay que esperar antes de intentar conectarse al servicio SCEP.
Tamaño de clave	Esta configuración especifica el tamaño de clave para el certificado.
Uso de la clave	Esta configuración especifica las operaciones criptográficas que se pueden realizar con la clave pública que está incluida en el certificado.
Uso extendido de la clave	Esta configuración especifica la finalidad de la clave que está incluida en el certificado.
Almacenamiento de claves de SCEP	Esta configuración especifica la ubicación de almacenamiento de la clave privada.
Función hash	Esta configuración especifica la función hash que un dispositivo con Windows 10 utiliza para la solicitud de inscripción de certificados.

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

BlackBerry Dynamics: configuración del perfil de SCEP

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

BlackBerry Dynamics: configuración del perfil SCEP	Descripción
Asunto	Esta configuración especifica el asunto del certificado, si es necesario para la configuración SCEP de la empresa. Escriba el asunto en el formato "/CN=<*common_name*>/O=<*domain_name*>". Si el perfil es para varios usuarios, puede utilizar una variable como, por ejemplo: %UserDistinguishedName%.
Tipo de SAN	Esta configuración especifica el tipo de nombre alternativo del asunto del certificado, si es necesario.
Valor de SAN	Esta configuración especifica la representación alternativa del asunto del certificado. El valor debe ser una dirección de correo, el nombre DNS del servidor CA, la URL completa del servidor o el nombre principal. El ajuste "Tipo de SAN" determina el valor adecuado que se debe especificar. Si se establece en "Nombre de RFC822" el valor debe ser una dirección de correo válida. Si se establece en "URI", el valor debe ser una URL válida que incluya el protocolo y la dirección IP o FQDN. Si se establece en "Nombre principal de NT", el valor debe ser un nombre principal válido. Si se establece en "Nombre de DNS", el valor debe ser un FQDN válido.
Algoritmo de clave	Esta configuración especifica el algoritmo que un dispositivo debe utilizar para generar el par de claves del cliente. Debe seleccionar un algoritmo que sea compatible con su CA.
Intensidad de RSA	Esta configuración especifica la intensidad de RSA utilizada para generar el par de claves del cliente. Debe introducir una intensidad de la clave que sea compatible con su CA. Esta configuración solo es válida si la opción "Algoritmo de clave" se establece en "RSA".

BlackBerry Dynamics: configuración del perfil SCEP	Descripción
Algoritmo de cifrado	Esta configuración especifica el algoritmo de cifrado utilizado para la solicitud de inscripción de certificados.
Función hash	Esta configuración especifica la función hash utilizada para la solicitud de inscripción de certificados.
Huella digital de certificado	Esta configuración especifica el hash de cifrado hexadecimal del certificado raíz para la autoridad de certificación. Puede utilizar uno de los siguientes algoritmos para especificar la huella digital: SHA-1, SHA-224, SHA-256, SHA-384 y SHA-512. MD5 solo es compatible si "Activar FIPS" no está seleccionado en el perfil BlackBerry Dynamics.
Renovación automática	Esta configuración especifica cuántos días antes de que caduque el certificado debe realizarse la renovación automática.
Uso de la clave	Esta configuración especifica las operaciones criptográficas que se pueden realizar con la clave pública que está incluida en el certificado.
Uso extendido de la clave	Esta configuración especifica la finalidad de la clave que está incluida en el certificado.
Restricciones de aplicaciones	En la configuración se especifican las aplicaciones de BlackBerry Dynamics que pueden utilizar el certificado.
Aplicaciones con permiso para utilizar SCEP	En la configuración se especifican las aplicaciones de BlackBerry Dynamics que pueden utilizar certificados SCEP. Esta configuración es válida únicamente si la opción "Restricciones de aplicación" se establece en "Permitir que las aplicaciones especificadas utilicen certificados".
Eliminar certificados caducados	Esta configuración especifica si el dispositivo debe borrar los certificados caducados.
Eliminar certificados duplicados	Esta configuración especifica si el dispositivo debe borrar los certificados duplicados. El dispositivo elimina el certificado que tiene la fecha de inicio más inmediata.

Envío del mismo certificado de cliente a varios dispositivos

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

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

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

1. En la barra de menús, haga clic en **Políticas y perfiles > Certificados > Certificado compartido**.

2. Haga clic en +.
3. Escriba un nombre y una descripción para el perfil.
4. En el campo **Contraseña**, escriba una contraseña para el perfil de certificado compartido.
5. En el campo **Archivo de certificado**, haga clic en **Examinar** para ubicar el archivo de certificado.
6. Si gestiona dispositivos Android Enterprise y desea evitar que los usuarios seleccionen el certificado para utilizarlo con otros fines, en la pestaña **Android** seleccione **Ocultar certificado en dispositivos Android Enterprise**.
7. Si gestiona dispositivos macOS, en la pestaña **macOS**, en la lista desplegable **Aplicar perfil a**, seleccione **Usuario** o **Dispositivo**.
8. Haga clic en **Agregar**.

Después de terminar: Asigne el perfil de certificado compartido a cuentas de usuarios, grupos de usuarios o grupos de dispositivos.

Especificación del certificado que usa una aplicación mediante un perfil de asignación de certificados

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

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

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

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

1. En la barra de menús, haga clic en **Políticas y perfiles > Certificados > Asignación de certificados**.
2. Haga clic en +.
3. Escriba un nombre y una descripción para el perfil.
4. En la tabla de asignación, haga clic en +.
5. En **URI de destino**, seleccione una de las siguientes opciones:
   - Seleccione **Ninguno** si la aplicación no utiliza el certificado para autenticar una conexión con un recurso.
   - Seleccione **Cualquiera** si la aplicación puede utilizar el certificado para autenticar una conexión con cualquier recurso.
   - Seleccione **Host especificado: puerto** y escriba el host y el puerto si la aplicación puede utilizar el certificado para autenticar una conexión con un recurso específico.
6. En **Certificado de la aplicación**, lleve a cabo una de las acciones siguientes:
   - Para especificar que la aplicación debe utilizar un certificado enviado al dispositivo por otro perfil, seleccione **Certificado seleccionado** y haga clic en el nombre del perfil en la lista desplegable.
   - Para especificar que la aplicación debe utilizar un certificado enviado al dispositivo por un tercero, seleccione **Alias de certificado** y escriba el alias del certificado.
   - Para especificar que la aplicación debe utilizar un certificado enviado al dispositivo por otro perfil, seleccione **Certificado seleccionado** y haga clic en el nombre del perfil en la lista desplegable.
7. En **Aplicaciones con permiso para el URI de destino**, lleve a cabo una de las siguientes acciones:

- Para permitir que cualquier aplicación gestionada pueda solicitar el certificado especificado, seleccione **Cualquier aplicación del espacio de trabajo**.
- Para permitir que únicamente las aplicaciones especificadas soliciten el certificado, seleccione **Aplicaciones especificadas** y haga clic en + para especificar una o varias aplicaciones.

8. Si fuera necesario, repita los pasos de 5 a 8 para agregar asignaciones adicionales al perfil.
9. Haga clic en **Agregar**.

Después de terminar:

- Asigne el perfil a las cuentas de usuario y los grupos de usuarios.
- Si crea más de un perfil de asignación de certificados, clasifique los perfiles según sea necesario. Seleccione un perfil y haga clic en ↓↑ para moverlo hacia arriba o hacia abajo en la clasificación. Haga clic en **Guardar**.

Administración de certificados de cliente para cuentas de usuarios

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

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

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

Adición y gestión de un certificado de cliente para una cuenta de usuario

1. En la barra de menús de la consola de administración, haga clic en **Usuarios > Dispositivos gestionados**.
2. Busque una cuenta de usuario y haga clic en ella.
3. Efectúe una de las acciones siguientes:

Tarea	Pasos
Adición de un certificado de cliente a una cuenta de usuario	Puede agregar un certificado de cliente a una cuenta de usuario individual y enviar el certificado a dispositivos con BlackBerry Dynamics u otros dispositivos gestionados iOS y Android. Añada certificados de cliente a cuentas de usuario cuando los dispositivos de usuarios necesiten certificados para S/MIME o autenticación de cliente y el certificado no se pueda enviar a los dispositivos a través de un perfil de credenciales de usuario o perfil SCEP. El certificado de cliente debe tener una extensión de nombre de archivo .pfx o p12. Puede enviar más de un certificado de cliente a los dispositivos. También puede utilizar los perfiles de credenciales de usuario para cargar certificados para usuarios individuales. Los perfiles de credenciales de usuario se pueden asociar a un perfil de Wi-Fi, VPN o correo. **a.** En la sección **Política de TI y perfiles**, haga clic en +. **b.** Haga clic en **Certificado de usuario**. **c.** Escriba una descripción para el certificado. **d.** En la sección **Aplicar certificado a**, seleccione una de las opciones siguientes: 1. **Otros dispositivos gestionados**: seleccione esta opción para enviar el certificado a dispositivos iOS y Android para todos los usos admitidos excepto para aplicaciones de BlackBerry Dynamics. 2. **Dispositivos con BlackBerry Dynamics**: seleccione esta opción para enviar el certificado a dispositivos para utilizarlo con aplicaciones de BlackBerry Dynamics. **e.** En el campo **Archivo de certificado**, haga clic en **Examinar**. Navegue al archivo de certificado y selecciónelo. **f.** Si ha seleccionado **Otros dispositivos gestionados**, en el campo **Contraseña**, escriba una contraseña para el certificado. Para dispositivos de iOS, se requiere una contraseña. Para los dispositivos Android, no es necesario proporcionar una contraseña si el dispositivo dispone de la última versión de UEM Client. Si no establece una contraseña, el usuario debe introducir la contraseña del dispositivo. **g.** Haga clic en **Agregar**. **h.** Configuración de un periodo de validez de los certificados de cliente. La vida predeterminada hasta que se eliminan los certificados de cliente es de 24 horas. 1. En la barra de menú, haga clic en **Configuración > Configuración general > Certificados**. 2. Especifique el periodo de validez para certificados PKCS#12 en el servidor.

Tarea	Pasos
Renovación o eliminación de un certificado de BlackBerry Dynamics para una cuenta de usuario	Puede enviar un comando al dispositivo de un usuario para solicitar la renovación del certificado de la entidad de certificación. También puede eliminar un certificado de BlackBerry Dynamics del dispositivo de un usuario. Si elimina un certificado, el conector de PKI de BlackBerry Dynamics envía una notificación a la entidad de certificación de que el certificado ya no está en uso, aunque el certificado no se revoca automáticamente. En la sección **Certificados de usuario**, realice una de las siguientes acciones: **a.** Haga clic en ↻ para solicitar la renovación del certificado de la entidad de certificación. **b.** Haga clic en ✕ para eliminar el certificado de los dispositivos del usuario. Para eliminar una credencial inteligente de Entrust de un dispositivo, el usuario también debe desactivar la credencial inteligente en BlackBerry UEM Client.
Adición de un certificado de cliente a un perfil de credenciales de usuario	Puede cargar certificados para usuarios individuales a un perfil de credenciales de usuario. Los usuarios también pueden cargar su certificado al perfil de credenciales de usuario mediante UEM Self-Service. La carga de certificados en perfiles de credenciales de usuario es compatible con dispositivos con iOS y para dispositivos con Android Enterprise. El certificado de cliente debe tener una extensión de nombre de archivo .pfx o p12. Si se carga un certificado nuevo al perfil de credenciales de usuario, se sustituye el certificado existente en los dispositivos de usuario. **Antes de empezar:** • Cree un perfil de credenciales de usuario para cargar manualmente los certificados. • Asigne el perfil de credenciales de usuario a los usuarios. **a.** En la sección **Política de TI y perfiles**, junto al perfil de credenciales de usuario, haga clic en **Agregar certificado**. **b.** Haga clic en **Examinar**. Navegue al certificado y selecciónelo. **c.** Introduzca la contraseña del certificado. Para dispositivos iOS, se requiere la contraseña. Para los dispositivos Android, no es necesario proporcionar la contraseña en UEM si el dispositivo dispone de la última versión de UEM Client. Si no especifica la contraseña, el usuario debe introducir la contraseña del dispositivo. **d.** Haga clic en **Agregar**.

Tarea	Pasos
Cambiar un certificado de cliente por un perfil de credenciales de usuario	El nuevo certificado sustituirá el certificado existente en el dispositivo. **a.** En la sección **Política de TI y perfiles**, junto al perfil de credenciales de usuario, haga clic en **Actualizar**. **b.** Haga clic en **Examinar** para buscar el certificado. **c.** Introduzca la contraseña del certificado. Para dispositivos iOS, se requiere la contraseña. Para dispositivos Android, no es necesario proporcionar la contraseña en UEM si el dispositivo dispone de la última versión de UEM Client. Si no especifica la contraseña, el usuario debe introducir la contraseña del dispositivo. **d.** Haga clic en **Guardar**.

Aviso legal

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