



BlackBerry Enterprise Identity

Guía de administración

Contents

¿En qué consiste BlackBerry Enterprise Identity ?.....	5
Uso de Enterprise Identity por primera vez.....	6
Descripción de los servicios, las autorizaciones y los grupos.....	7
Administración de servicios.....	8
Gestión de servicios de la consola de administración de BlackBerry UEM.....	8
Visualización de una lista de plantillas de servicio de la consola de BlackBerry UEM.....	8
Ver una lista de servicios personalizados que haya creado en la consola de BlackBerry UEM.....	8
Creación de un servicio SaaS de la consola de BlackBerry UEM.....	8
Adición de un servicio de Proveedor de notificaciones de ADFS.....	10
Adición de un servicio personalizado en la consola de BlackBerry UEM.....	13
Cambio de un servicio activo de la consola de BlackBerry UEM.....	13
Eliminación de un servicio de la consola de BlackBerry UEM.....	13
Visualización de las opciones de configuración de SAML de la consola de BlackBerry UEM.....	13
Exportación de metadatos de servicio SAML en la consola de BlackBerry UEM.....	14
Adición de una aplicación de OpenID Connect.....	14
Inicio de sesión en la consola de BlackBerry Enterprise Identity.....	14
Administración de los niveles de autenticación.....	16
Activación de la autenticación de dos factores.....	16
Activación de Mobile ZSO.....	17
Activación de Mobile ZSO en BlackBerry UEM.....	17
Administración de los factores de riesgo.....	18
Configuración del factor de riesgo de detección de red.....	18
Administración de políticas de autenticación.....	20
Creación de una política de autenticación de Enterprise Identity.....	20
Asignación de una política de Enterprise Identity a un grupo de usuarios.....	21
Eliminación de una política de Enterprise Identity.....	21
Uso de la clasificación del nivel del autenticador y de las políticas de autenticación para administrar la seguridad.....	22
Solicitud de autenticación adicional cuando los usuarios se conectan a una red externa.....	22
Configuración de la clasificación de autenticador.....	22
Adición de una política de autenticación para redes externas.....	22
Solicitud de autenticación adicional cuando los usuarios utilizan un navegador por primera vez.....	23

Configuración de la clasificación de autenticador.....	23
Adición de una política de autenticación para la primera vez que los usuarios utilizan un navegador.....	23
Activación de la autenticación de los usuarios con PingFederate.....	24
Creación de un cliente de Ping Identity en un servidor de PingFederate.....	24
Configuración de un proveedor de identidad en BlackBerry UEM.....	25
Creación de una política de BlackBerry Enterprise Identity para usuarios de PingFederate.....	25
Activación de la autenticación de los usuarios con Okta.....	26
Creación de una aplicación Okta.....	26
Configuración de Okta como un proveedor de identidad en BlackBerry UEM.....	28
Administración de grupos de aplicaciones.....	30
Asignación de autorizaciones a usuarios o grupos.....	31
Cambio de la configuración de Enterprise Identity.....	32
Personalización de la página de inicio de sesión de usuario de su empresa....	33
Compatibilidad de SAML ECP para Microsoft Office 365.....	34
Activación de la compatibilidad de ECP para Office 365.....	34
Cómo impedir que los usuarios sean bloqueados en sus cuentas.....	35
Selección de inquilino y dominio.....	36
Gestión de inquilinos de BlackBerry UEM en la consola de BlackBerry Enterprise Identity.....	37
Gestión de administradores y usuarios.....	38
Creación de un administrador de Enterprise Identity personalizado.....	38
Aviso legal.....	39

¿En qué consiste BlackBerry Enterprise Identity ?

BlackBerry Enterprise Identity proporciona autenticación para algunas aplicaciones web de BlackBerry, como la consola de gestión de BlackBerry UEM Cloud y BlackBerry Persona Mobile. BlackBerry Enterprise Identity también ofrece el registro único (SSO) a los servicios en la nube, como Microsoft Office 365, G Suite y BlackBerry Workspaces, entre otros. Con el inicio de sesión único, los usuarios no tienen que realizar varios inicios de sesión ni recordar varias contraseñas. Los administradores también pueden agregar servicios personalizados a Enterprise Identity para ofrecer a los usuarios acceso a las aplicaciones internas. Los usuarios pueden acceder a los servicios desde cualquier dispositivo que deseen usar, como los dispositivos iOS, Android o BlackBerry 10, y otras plataformas informáticas.

Enterprise Identity Se instala junto con BlackBerry UEM y BlackBerry UEM Cloud. Los administradores pueden usar la consola de BlackBerry UEM Cloud o de BlackBerry UEM para agregar servicios, administrar usuarios, y agregar y gestionar administradores adicionales. La integración con los productos EMM de BlackBerry facilita la administración de los usuarios y les permite acceder a los servicios en la nube desde sus dispositivos.

Para utilizar Enterprise Identity, debe adquirir licencias de usuario de las ediciones Collaboration, Application o Content de BlackBerry Enterprise Mobility Suite, o licencias de usuario de BlackBerry Enterprise Identity independientes. Para obtener más información acerca de BlackBerry Enterprise Identity, incluido cómo comprar Enterprise Identity, consulte blackberry.com.

Los siguientes navegadores son compatibles para la administración: Internet Explorer 11, Google Chrome, Mozilla Firefox y Safari. El uso de clientes es compatible con todos los navegadores mencionados anteriormente, así como con los navegadores nativos de los dispositivos que ejecutan BlackBerry 10 OS versión 10.2.1 o posterior, iOS 8 o posterior y Android OS 4.0 o posterior.

Función	Ventaja
Mejora de la productividad de los empleados	Los empleados pueden usar una contraseña para todos los servicios en la nube, en todos los dispositivos móviles (iOS, Android y BlackBerry) y las plataformas informáticas tradicionales (Windows y macOS). De este modo se elimina la frustración de usar varias contraseñas e inicios de sesión.
Personalización de la autenticación	En función de su escenario de seguridad, BlackBerry Enterprise Identity le permite elegir el método de autenticación para un determinado servicio, grupo de usuarios o una combinación de ambos. Incluso puede adaptar las políticas de la empresa según las situaciones de alto riesgo.
Agilización de la estrategia móvil	Los usuarios y sus identidades son fundamentales para la movilidad empresarial. BlackBerry Enterprise Identity unifica y simplifica el acceso a los servicios en la nube, como Microsoft Office 365, Salesforce, Google Apps, BlackBerry Workspaces o la mayoría de las aplicaciones y servicios basados en SAML, lo que respalda la productividad de la plantilla móvil cada vez mayor.
Aprovechamiento de la solución de EMM existente desde BlackBerry	Enterprise Identity se ha integrado plenamente en BlackBerry UEM y ofrece EMM líder del sector, junto con un mayor control de acceso a todos los servicios en la nube. De este modo, puede acceder a funciones como el aprovisionamiento de aplicaciones con un solo clic y el derecho al inicio de sesión único, BlackBerry 2FA y el inicio de sesión cero móvil (Mobile ZSO).

Uso de Enterprise Identity por primera vez

BlackBerry UEM, y BlackBerry UEM Cloud que incluya el software BlackBerry Enterprise Identity. En BlackBerry UEM versión 12.7 MR1 y posterior, no necesita activar Enterprise Identity. Si la empresa dispone de las licencias adecuadas, Enterprise Identity se activará automáticamente.

Descripción de los servicios, las autorizaciones y los grupos

Los servicios son aplicaciones, a menudo ubicadas en la nube, a las que los usuarios necesitan acceder. Por ejemplo, Microsoft Office 365, BlackBerry Workspaces, o WebEx. Al configurar un servicio en BlackBerry UEM, BlackBerry UEM Cloud o BlackBerry Enterprise Identity, puede establecer una interfaz segura entre Enterprise Identity y la instancia o el inquilino de dicho servicio. Después de utilizar BlackBerry UEM o BlackBerry UEM Cloud para agregar un servicio, puede utilizar la consola de administración de BlackBerry UEM para administrar el servicio e implementar los derechos del servicio para los usuarios.

La manera más eficiente de autorizar a los usuarios es mediante los grupos de aplicaciones. Un grupo de aplicaciones puede combinar la autorización de SSO para un servicio y las aplicaciones del cliente que los dispositivos necesitan para interactuar con el servicio. Puede asignar grupos de aplicaciones a usuarios o grupos de usuarios, con el objetivo de ofrecerles todo lo que necesitan para acceder al servicio.

Los grupos de usuarios aportan flexibilidad a los administradores a la hora de conceder autorizaciones a un gran número de usuarios a la vez, en lugar de realizar la autorización manualmente a medida que los usuarios se añadan o se eliminen del grupo. Cuando se añade un usuario al grupo, la autorización se asigna automáticamente, lo que le permite acceder al servicio desde cualquier dispositivo utilizando las mismas credenciales. Si se elimina un usuario del grupo, este deja de tener acceso al servicio automáticamente. También se pueden asignar autorizaciones para el servicio a usuarios individuales si es necesario.

Plazo	Descripción
Servicio	Los servicios incluyen Workspaces, Box, Workday, WebEx, Salesforce y otros, incluidos servicios personalizados.
Autorización	Una autorización es una asignación de servicio llevada a cabo con BlackBerry UEM que le indica a Enterprise Identity que debe proporcionar acceso de inicio de sesión único a un servicio determinado a un usuario o un grupo concreto.
Grupo de aplicaciones	Un grupo de aplicaciones es un conjunto de aplicaciones que puede incluir la autorización con inicio de sesión único y los archivos binarios asociados para los dispositivos móviles.
Usuario	Un usuario es un usuario de BlackBerry UEM.
Grupo de usuarios	Un grupo de usuarios es un conjunto de usuarios de BlackBerry UEM.

Administración de servicios

Si está utilizando BlackBerry UEM 12.7.x y versiones posteriores o BlackBerry UEM Cloud, utilice la consola de administración de BlackBerry UEM para administrar los servicios de su empresa.

Gestión de servicios de la consola de administración de BlackBerry UEM

Antes de configurar servicios de SaaS u otros servicios en la consola de administración de BlackBerry UEM, su administrador del sistema debe agregar el servicio. Para obtener más información, [consulte el contenido sobre integración de los servicios de SaaS](#).

Cuando su empresa haya adquirido las licencias adecuadas para BlackBerry Enterprise Identity (para obtener más información, consulte la [Guía de licencias de BlackBerry UEM](#)), podrá utilizar la consola de BlackBerry UEM para administrar los servicios y las funciones de dichos servicios. La adición de los servicios requiere la configuración de la seguridad y de otros parámetros específicos de su empresa.

Después de agregar un servicio, en la consola de administración de BlackBerry UEM puede autorizar a los usuarios para utilizar el servicio en función del usuario o a través de un grupo. Puede cambiar la configuración del servicio en la consola de administración de BlackBerry UEM.

Visualización de una lista de plantillas de servicio de la consola de BlackBerry UEM

1. En la consola de gestión de BlackBerry UEM, en la barra de menú, haga clic en **Configuración**.
2. Haga clic en **BlackBerry Enterprise Identity > Servicios**.
3. Haga clic en **+**.

Aparece la lista de plantillas de servicio disponibles.

Ver una lista de servicios personalizados que haya creado en la consola de BlackBerry UEM

1. En la consola de gestión de BlackBerry UEM, en la barra de menú, haga clic en **Configuración**.
2. Haga clic en **BlackBerry Enterprise Identity > Servicios**.

Aparece la lista de servicios personalizados.

Creación de un servicio SaaS de la consola de BlackBerry UEM

Nota: Si desea crear dos instancias del mismo tipo de servicio en BlackBerry UEM (por ejemplo, Box), debe proporcionar distintos ID de entidad del proveedor de servicios para cada instancia.

1. En la consola de administración de BlackBerry UEM, en la barra de menú, haga clic en **Configuración**.
2. Haga clic en **BlackBerry Enterprise Identity > Servicios**.
3. Haga clic en **+**.
4. Seleccione el tipo de servicio que desea crear (por ejemplo, Box).
5. En la pantalla **Agregar un servicio de BlackBerry Enterprise Identity**, introduzca los metadatos del proveedor de servicios. Estos metadatos son específicos del proveedor de servicios y de su empresa. Tenga en cuenta que solo aparecen los campos que están asociados a la plantilla de servicio seleccionada.

Nombre	Descripción
Inicio de sesión cero móvil	Seleccione esta opción si desea activar el inicio de sesión cero móvil.
Nombre	Introduzca el nombre del proveedor de SaaS.
Descripción	La descripción del inquilino es opcional.
Logotipo	Agregue un logotipo para asociarlo al servicio.
ID de entidad del proveedor de servicios	Introduzca la URL o el nombre único que usa para acceder a los servicios SaaS.
URL de POST del servicio de consumidor de aserción	Introduzca la POST URL proporcionada por el proveedor de servicios.
Asistencia para inicios de sesión realizados mediante IdP	Introduzca el tipo de asistencia para inicio de sesión que requiera su empresa.
Opciones de firma	Introduzca su elección de aserción.
Certificado de firma mediante IDP	Introduzca el certificado x509 compartido con el proveedor de servicios.
Clave privada de firma mediante IDP	Introduzca la clave x509 para el certificado de firma correspondiente. Consérvela de forma segura.
Certificado de cifrado	Introduzca el certificado de cifrado
Información de servicios específicos	Algunos servicios requieren información adicional o información diferente a la de estas descripciones. La mayoría de las veces, esta información adicional está preconfigurada.
Notificación: atributo del identificador de nombre	Seleccione el atributo identificador de la notificación.

Nombre	Descripción
Atributos de notificación de SAML	<ul style="list-style-type: none"> Nombre: introduzca un nombre para la notificación de SAML Atributo de SAML: introduzca el atributo de SAML Tipo de notificación de SAML <ul style="list-style-type: none"> Local: si elige una notificación local, tiene que seleccionar la opción en la lista de valor de atributo. Este asignará un atributo de SAML a un tipo de atributo conocido para BlackBerry Enterprise Identity, como Nombre de usuario. Estático: si elige una notificación estática, tiene que escribir una opción en el campo Valor de atributo. Directorio: si elige Directorio, puede escribir el nombre de un atributo de Active Directory. Los valores que coinciden con el texto que escribe se sugieren automáticamente. Valor de atributo: seleccione o escriba un valor de atributo. Se trata de un valor de atributo definido que el servicio SaaS puede solicitar para configurar el servicio para los usuarios de su empresa. Tipo de atributo: seleccione un tipo para el atributo. El tipo se basa en los requisitos del servicio SaaS. El valor predeterminado es anyType. Opcionalmente, si desea que el atributo sea necesario, seleccione la casilla de verificación Obligatorio.

6. Haga clic en **Guardar**.

Adición de un servicio de Proveedor de notificaciones de ADFS

Si su empresa tiene aplicaciones que utilizan la autenticación basada en formularios de servicios de federación de Active Directory (ADFS), puede añadir un servicio de Proveedor de notificaciones de ADFS de forma que Enterprise Identity pueda autenticarse en las aplicaciones de ADFS utilizando el tipo de autenticación de formularios.

Enterprise Identity es compatible con ADFS 2019 y posterior

Antes de empezar:

- Compruebe que la función de ADFS se ha agregado al servidor de Active Directory.
 - Compruebe que UEM esté conectado al servidor de Active Directory que tiene la función de ADFS.
1. En la consola de gestión de UEM, haga clic en **Configuración > BlackBerry Enterprise Identity > Servicios**.
 2. En la tabla **Servicios SAML**, haga clic en **+**.
 3. Haga clic en **Proveedor de notificaciones de ADFS**.
 4. Si quiere activar ZSO para los usuarios, seleccione las casillas de verificación **Permitir Mobile ZSO cuando lo especifique la política de autenticación** y **Permitir Kerberos Desktop ZSO cuando lo especifique la política de autenticación**.
 5. Escriba un nombre y una descripción para el servicio.
 6. En el campo **ID de entidad del proveedor de servicios**, introduzca `http://<adfs_endpoint>/adfs/services/trust`, siendo *adfs_endpoint* el nombre del servidor de Active Directory que tenga la función de ADFS.
 7. En el campo **URL de POST del servicio de consumidor de aserción**, introduzca `http://<adfs_endpoint>/adfs/services/ls`, donde *adfs_endpoint* es el nombre del servidor de Active Directory que tiene la función de ADFS.

- En el campo **URL del servicio de cierre de sesión único**, introduzca `http://<adfs_endpoint>/adfs/services/ls`, donde `adfs_endpoint` es el nombre del servidor de Active Directory que tiene la función de ADFS.
- Haga clic en **Guardar**.

Después de terminar: Asigne el servicio a los usuarios.

Configuración del Proveedor de notificaciones en AD-FS

Antes de empezar: [Adición de un servicio de Proveedor de notificaciones de ADFS](#)

- En la consola de gestión de UEM, haga clic en **Configuración > BlackBerry Enterprise Identity > Servicios**.
- En la tabla **Servicios SAML**, haga clic en el servicio Proveedor de notificaciones en ADFS.
- En la sección **Metadatos del servicio SAML**, haga clic en el enlace para descargar los metadatos del servicio SAML. Copie el archivo en el servidor de Windows que ejecuta ADFS.
- Abra el administrador de ADFS.
- En el panel izquierdo, haga clic en **Confianzas de proveedores de notificaciones**.
- En el panel derecho, haga clic en **Agregar proveedor de notificaciones**.
- En **Asistente de confianzas de proveedores de notificaciones**, haga clic en **Iniciar > Siguiente**.
- Seleccione **Importar datos sobre el proveedor de notificaciones del archivo** y abra el archivo de metadatos que descargó en el paso 3. Haga clic en **Siguiente**.
- Escriba un nombre y una descripción para la Confianza de proveedores de notificaciones. Haga clic en **Siguiente** hasta que aparezca el botón Guardar.
- Haga clic en **Guardar**.

Si quiere comprobar su configuración de ADFS, puede crear una aplicación de prueba utilizando Claims X-Ray. Para obtener más información, consulte <https://adfs-help.microsoft.com/ClaimsXray/TokenRequest>.

Uso de Enterprise Identity como proveedor de notificaciones predeterminado

Para utilizar Enterprise Identity como proveedor de notificaciones predeterminado, puede ejecutar el siguiente comando en Windows PowerShell. Cuando Enterprise Identity es el proveedor de notificaciones predeterminado, no se solicita a los usuarios que se autenticuen cuando acceden a un servicio.

En Windows PowerShell, introduzca el siguiente comando:

```
Set-AdfsRelyingPartyTrust -TargetName <relying_party_name> -ClaimsProviderName @("<claims_provider_display_name>")
```

Ejemplo: Configuración de la asignación de notificaciones para Office 365

En los pasos siguientes, se proporciona un ejemplo de cómo configurar la asignación básica de notificaciones para Microsoft Office 365. Su organización puede tener diferentes requisitos de asignación de notificaciones.

Antes de empezar: [Uso de Enterprise Identity como proveedor de notificaciones predeterminado](#).

- En el administrador de ADFS, haga clic en **Editar reglas de notificación** para el proveedor de notificaciones Enterprise Identity que ha configurado.
- Haga clic en **Agregar regla>Enviar notificaciones mediante una función personalizada**.
- En la ventana de la plantilla de regla **Seleccionar regla**, en la lista desplegable **Plantilla de regla de notificación**, seleccione **Enviar notificaciones mediante una regla personalizada**. Haga clic en **Siguiente**.
- En la ventana **Configurar regla**, en el campo **Nombre de regla de notificación**, escriba `Pasar todas las notificaciones`.

5. En el panel **Regla personalizada**, introduzca lo siguiente:

```
c:[ ]
    => issue(claim = c);
```

6. Haga clic en **Finalizar**.

7. En la ventana **Configurar regla**, en el campo **Nombre de regla de notificación**, escriba `Transformar UPN`.

8. En el panel **Regla personalizada**, introduzca lo siguiente:

```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn" ]
=> issue(Type = "http://schemas.xmlsoap.org/claims/UPN", Issuer =
c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = regexreplace(c.Value,
"^(?<user>.*)$", "${user}<domain_suffix_for_your_users>"), ValueType =
c.ValueType);
```

Donde el sufijo del dominio es el dominio de correo electrónico de los usuarios (por ejemplo `"${user}@example.com"`).

9. Haga clic en **Finalizar**.

10. En la consola de gestión de UEM, haga clic en **Configuración > BlackBerry Enterprise Identity > Servicios**.

11. En la tabla **Servicios SAML**, haga clic en el servicio ADFS que ha creado.

12. En **Notificaciones**, en la lista desplegable **Atributo del identificador de nombre**, seleccione **ID inmutable**.

13. En la tabla de atributos de notificación de SAML, haga clic en **+**. Siga estas instrucciones:

- En el campo **Nombre**, escriba `Nombre de usuario`.
- En **Atributo de SAML**, seleccione `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name`.
- Establezca el tipo de notificación de SAML en **Local**.
- Establezca el valor del atributo en el nombre que introdujo para el atributo de notificación (por ejemplo, `Nombre de usuario`).
- Establezca el valor del atributo en **anyType**.
- Haga clic en **Guardar**.

14. En la tabla de atributos de notificación de SAML, haga clic en **+**. Siga estas instrucciones:

- En el campo **Nombre**, escriba `UPN`.
- En **Atributo de SAML**, seleccione `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn`.
- Establezca el tipo de notificación de SAML en **Local**.
- Establezca el valor del atributo en el nombre que introdujo para el atributo de notificación (por ejemplo, `UPN`).
- Establezca el valor del atributo en **anyType**.
- Haga clic en **Guardar**.

15. En la tabla de atributos de notificación de SAML, haga clic en **+**. Siga estas instrucciones:

- En el campo **Nombre**, escriba `ID inmutable`.
- En **Atributo de SAML**, seleccione `http://schemas.microsoft.com/LiveID/Federation/2008/05/ImmutableID`.
- Establezca el tipo de notificación de SAML en **Local**.
- Establezca el valor del atributo en el nombre que introdujo para el atributo de notificación (por ejemplo, `ID inmutable`).
- Establezca el valor del atributo en **anyType**.

16. Haga clic en **Guardar**.

Adición de un servicio personalizado en la consola de BlackBerry UEM

BlackBerry proporciona una creciente selección de plantillas de servicios predefinidas. Como administrador, es posible que quiera agregar servicios personalizados a BlackBerry Enterprise Identity. Pueden integrarse la mayoría de los servicios que utilizan los protocolos SAML 2.0. Los servicios de SAML que integre pueden personalizarse y pueden ser específicos para su empresa, o puede elegir integrar un servicio desde un proveedor de SaaS con un uso más amplio.

Cuando se activa un servicio, los usuarios autorizados pueden utilizarlo. Cuando se desactiva un servicio, todos los usuarios autorizados dejan de tener acceso hasta que se activa de nuevo.

Para obtener información detallada sobre las plantillas de servicio disponibles, consulte [Integración de servicios SaaS](#).

1. En la consola de gestión de BlackBerry UEM, en la barra de menú, haga clic en **Configuración**.
2. Haga clic en **BlackBerry Enterprise Identity > Servicios**.
3. Haga clic en **+**.
4. Seleccione **Servicio personalizado**.
5. Complete los campos para configurar el servicio personalizado.
 - Al agregar una notificación de SAML, si elige una notificación local, tiene que seleccionar la opción en la lista de valor de atributo. Este asignará un atributo de SAML a un tipo de atributo conocido para BlackBerry Enterprise Identity, como Nombre de usuario.
 - Al agregar una notificación de SAML, si elige una notificación estática, tiene que escribir la opción en el campo de valor de atributo.
6. Haga clic en **Guardar**.

Cambio de un servicio activo de la consola de BlackBerry UEM

1. En la consola de administración de BlackBerry UEM, en la barra de menú, haga clic en **Configuración**.
2. Haga clic en **BlackBerry Enterprise Identity > Servicios**.
3. Haga clic en el servicio que desea cambiar.
4. Para cambiar la configuración del servicio para un servicio o función editable, en la sección **Configuración del servicio**, complete los campos. Es posible que en algunos servicios no se permitan las ediciones.
5. Haga clic en **Guardar**.

Eliminación de un servicio de la consola de BlackBerry UEM

Antes de eliminar un servicio, debe eliminar todos los derechos de usuario de ese servicio en la consola de gestión de BlackBerry UEM.

1. En la consola de administración de BlackBerry UEM, en la barra de menú, haga clic en **Configuración**.
2. Haga clic en **BlackBerry Enterprise Identity > Servicios**.
3. Haga clic en la X junto al servicio que desea eliminar.
4. Haga clic en **Quitar**.

Visualización de las opciones de configuración de SAML de la consola de BlackBerry UEM

1. En la consola de administración de BlackBerry UEM, en la barra de menú, haga clic en **Configuración**.
2. Haga clic en **BlackBerry Enterprise Identity > Servicios**.
3. Haga clic en la configuración de servicio SaaS para ver la configuración de SAML.

Exportación de metadatos de servicio SAML en la consola de BlackBerry UEM

Es posible que necesite que los metadatos del servicio SAML configuren la interfaz segura entre BlackBerry Enterprise Identity y la instancia o el inquilino del servicio que está configurando (por ejemplo, Box).

1. En la consola de administración de BlackBerry UEM, en la barra de menú, haga clic en **Configuración**.
2. Haga clic en **BlackBerry Enterprise Identity > Servicios**.
3. Haga clic en la configuración de servicio SaaS para ver el encabezado de los metadatos de SAML.
4. Haga clic en el hipervínculo para descargar el archivo XML.

Adición de una aplicación de OpenID Connect

Puede añadir una aplicación de OpenID Connect que esté disponible para su empresa o inquilino de UEM. El administrador o desarrollador de aplicaciones es el encargado de hacer que las aplicaciones de OpenID Connect estén disponibles.

1. En la consola de gestión de BlackBerry UEM, en la barra de menús, haga clic en **Configuración**.
2. Haga clic en **BlackBerry Enterprise Identity > Servicios**.
3. En la tabla **Aplicaciones de OpenID Connect**, haga clic en +.
Se muestra una lista de las aplicaciones de OpenID Connect disponibles.
4. Seleccione una aplicación.
5. En la pantalla **Agregar un servicio de BlackBerry Enterprise Identity**, realice una de estas acciones:
 - Seleccione **Permitir Mobile ZSO cuando lo especifique la política de autenticación**
 - Seleccione **Permitir Kerberos Desktop ZSO cuando lo especifique la política de autenticación**.
6. Revise los ámbitos de la aplicación. Haga clic en **Guardar**.

Para editar la aplicación, haga clic en el nombre de la aplicación en la tabla Aplicaciones de OpenID Connect.

Actualización del consentimiento de una aplicación de OpenID Connect

Si los ámbitos requeridos para una aplicación de OpenID Connect cambian, debe actualizar el consentimiento de la aplicación. Cuando los ámbitos requeridos cambian, se muestra una notificación en la sección OpenID Connect de la página de servicios de BlackBerry Enterprise Identity.

1. En la consola de gestión de BlackBerry UEM, en la barra de menús, haga clic en **Configuración**.
2. Haga clic en **BlackBerry Enterprise Identity > Servicios**.
3. En la tabla de aplicaciones **OpenID Connect**, en la sección **Se requiere consentimiento**, haga clic en la notificación para una aplicación.
4. En el cuadro de diálogo **Actualizar aplicación**, revise los ámbitos o clientes que se han agregado o quitado. Haga clic en **Guardar**.

Eliminación de una aplicación de OpenID Connect

1. En la consola de administración de BlackBerry UEM, en la barra de menú, haga clic en **Configuración**.
2. Haga clic en **BlackBerry Enterprise Identity > Servicios**.
3. En la tabla **Aplicaciones OpenID Connect**, haga clic en X, ubicado junto a la aplicación que desee eliminar.
4. En el cuadro de diálogo **Retirar consentimiento**, haga clic en **Eliminar**.

Inicio de sesión en la consola de BlackBerry Enterprise Identity

Es posible que tenga que iniciar sesión en la consola de BlackBerry Enterprise Identity para realizar algunas tareas como la búsqueda en los registros del sistema.

Antes de empezar: Active las ventanas emergentes en su navegador.

1. En la consola de administración de BlackBerry UEM, haga clic en la opción **Aplicaciones** de la barra de menú.
2. Haga clic en **Enterprise Identity**. Aparece un mensaje que le solicita que sincronice los servicios de Enterprise Identity.
3. Haga clic en la consola **Open Enterprise Identity**. La consola de administrador se abre en una nueva pestaña del navegador. Si la consola no se abre, asegúrese de que ha activado los elementos emergentes en el navegador.
4. Cuando termine, cierre la pestaña del navegador.

Administración de los niveles de autenticación

Hay tres tipos de autenticación disponibles en Enterprise Identity. La clasificación de estos autenticadores puede modificarse con la consola de BlackBerry UEM, en la página **Configuración**. Para obtener más información sobre la clasificación, consulte [Modificación de la configuración de Enterprise Identity](#).

Tipo de autenticador	Descripción
Contraseña de empresa	Este método de seguridad requiere que los usuarios introduzcan una contraseña antes de acceder a un servicio. Es el método predeterminado. La contraseña está asociada actualmente a una cuenta de usuario en Active Directory, un directorio LDAP o BlackBerry UEM.
Contraseña de empresa y BlackBerry 2FA	Este método de seguridad aprovecha las capacidades de BlackBerry 2FA y requiere una contraseña y la confirmación por parte del dispositivo móvil del usuario antes de poder acceder a un servicio.
Mobile ZSO	Este método de seguridad, disponible en dispositivos móviles, permite al usuario acceder a un servicio sin necesidad de autenticarse explícitamente. En su lugar, considera la autenticación del usuario con el dispositivo o el contenedor de seguridad como prueba de su identidad.
Contraseña Ping	Este método de seguridad, disponible para usuarios de PingFederate requiere que los usuarios introduzcan su contraseña de Ping Identity antes de que puedan acceder a un servicio. Para más seguridad, también puede requerir a los usuarios que confirmen una solicitud o que introduzcan su PingID.

Puede asignar estos niveles de autenticación a un usuario o un grupo para cada servicio al definir una política de autenticación. Para obtener más información sobre las políticas, consulte [Administración de políticas de autenticación](#).

Activación de la autenticación de dos factores

La activación de la autenticación de dos factores implica activar BlackBerry 2FA, decidir su clasificación de autenticador y asignar una política de autenticación que requiera su nivel de autenticación.

Antes de empezar:

- Active [BlackBerry 2FA](#) en BlackBerry UEM y aplique el perfil de BlackBerry 2FA al usuario o el grupo.
 - Asegúrese de que los usuarios que necesitan usar BlackBerry 2FA dispongan de su dispositivo móvil y se hayan activado. Para obtener más información sobre la activación de dispositivos, [consulte el contenido referente a BlackBerry 2FA](#).
1. Asigne BlackBerry 2FA a un nivel de autenticación. Para obtener más información, consulte [Administración de los niveles de autenticación](#).
 2. Configure una política de autenticación que establezca BlackBerry 2FA como nivel de autenticación que un grupo de usuarios concreto o un servicio específico debe utilizar. Para obtener más información, consulte [Administración de las políticas de autenticación](#).

Activación de Mobile ZSO

Al activar el inicio de sesión cero móvil (Mobile ZSO), se activa para los servicios con los que desea utilizarlo, se decide su clasificación de autenticador y se asigna una política de autenticación que requiera su nivel de autenticación.

La activación de Mobile ZSO para un servicio hace posible que dicho servicio se autentique con el certificado de un dispositivo gestionado del usuario sin el uso de un nombre de contraseña ni contraseña.

Activación de Mobile ZSO en BlackBerry UEM

Antes de empezar:

- Los usuarios deben tener un dispositivo Android Enterprise activado con un perfil de trabajo, un dispositivo Samsung Knox, un dispositivo iOS o un dispositivo BlackBerry 10.
 - Los usuarios deben contar con BlackBerry Secure Connect Plus en sus dispositivos.
1. Inicie sesión en BlackBerry UEM como administrador.
 2. En la barra de menús, haga clic en **Configuración > BlackBerry Enterprise Identity > Servicios**.
 3. Haga clic en el servicio para el cual desea activar Mobile ZSO.
 4. Seleccione la opción **Permitir Mobile ZSO cuando lo especifique la política de autenticación**.
 5. Haga clic en **Guardar**.
 6. Asigne Mobile ZSO a un nivel de autenticación. Para obtener más información, consulte [Administración de los niveles de autenticación](#).
 7. Configure una política de autenticación que establezca Mobile ZSO como nivel de autenticación que un grupo de usuarios concreto o un servicio específico debe utilizar. Para obtener más información, consulte [Administración de las políticas de autenticación](#).

La activación del inicio de sesión cero móvil (Mobile ZSO) para un servicio permite que dicho servicio se autentique con Mobile ZSO. La política de autenticación general asignada en BlackBerry UEM debe permitir el uso de Mobile ZSO.

Si configura un servicio para usar Mobile ZSO sin un autenticador de reserva, solo resultará accesible a través de dispositivos móviles administrados. Sin embargo, si se configura un autenticador con contraseña de reserva, Mobile ZSO se utilizará en dispositivos móviles administrados, y el usuario podrá usar la contraseña en otros dispositivos.

Administración de los factores de riesgo

Los factores de riesgo son funciones opcionales en las directivas de autenticación que proporcionan una forma de equilibrar el nivel de autenticación según el riesgo. Cuando un usuario está en un navegador o en una red de confianza, podrá disfrutar de un acceso más sencillo a los servicios que necesita, pero puede aplicar una política de autenticación más estricta en otras circunstancias.

Factor de riesgo	Descripción
Detección de navegador	Este factor de riesgo pide a los usuarios que establezcan una referencia de confianza entre el navegador y Enterprise Identity la primera vez que abren un navegador. Después de que se haya establecido la confianza, los inicios de sesión posteriores pueden usar un nivel de autenticación más simple. Los usuarios pueden ver y eliminar las entradas de navegador de confianza en BlackBerry UEM Self-Service.
Detección de red	<p>Este factor de riesgo determina si la aplicación o el navegador de un usuario están conectados a la misma red que el servidor de BlackBerry UEM. Si no es así, se puede aplicar un nivel de autenticación mayor. Este factor de riesgo puede permitir a los usuarios que inicien sesión más fácilmente en determinados servicios cuando están en la red del trabajo. Para obtener más información acerca de la configuración de este factor de riesgo, consulte Configuración del factor de riesgo de detección de red.</p> <p>Si desea desactivar la detección de red de manera global, puede iniciar sesión en la consola de Enterprise Identity y desactivar la detección de red de trabajo en la lista de inquilinos de UEM.</p> <p>Nota: No puede activar el factor de riesgo de detección de red en BlackBerry UEM Cloud.</p>

Configuración del factor de riesgo de detección de red

Antes de empezar: No puede activar el factor de riesgo de detección de red en BlackBerry UEM Cloud.

1. En la consola de gestión de BlackBerry UEM, haga clic en **Configuración > BlackBerry Enterprise Identity > Configuración**.
2. Introduzca el nombre de host de la red del trabajo del servidor de BlackBerry UEM que usen sus equipos y dispositivos de trabajo. También puede introducir el nombre de grupo de DNS que resuelve varias direcciones IP del servidor de BlackBerry UEM.
3. Confirme que los equipos y los dispositivos de trabajo se pueden conectar al nombre de host mediante el número de puerto indicado. El factor de riesgo no funcionará si un firewall bloquea el puerto.
4. Haga clic en **Guardar**.
5. Haga clic en **Configuración > Infraestructura > Certificados del servidor > Certificado SSL para BlackBerry Web Services**.

Los navegadores y dispositivos del ordenador de trabajo deben confiar en el certificado cuando se conectan al nombre de host de la red de trabajo, y el certificado predeterminado es autofirmado y no es de confianza. Puede cargar un certificado BlackBerry Web Services de confianza en BlackBerry UEM.

Después de terminar: Es posible que algunos navegadores web requieran un certificado de confianza externo. Si es así, se puede cargar un nuevo certificado de BlackBerry Web Services en BlackBerry UEM. Haga clic en **Configuración > Infraestructura > Certificados del servidor > Certificado SSL para BlackBerry Web Services**.

Después de terminar: Cuando cree o edite una política de autenticación Enterprise Identity, haga clic en la casilla de verificación **Detección de red** con el fin de agregar el factor de riesgo. Para obtener más información acerca de la creación de políticas de autenticación, consulte [Creación de una política de autenticación de Enterprise Identity](#).

Administración de políticas de autenticación

Puede usar la consola de administración de BlackBerry UEM para crear, administrar y clasificar las políticas de autenticación. Las políticas se pueden anular según el servicio. Para obtener información general sobre las políticas y los perfiles, consulte las [políticas de TI](#), en el contenido referente a la administración de BlackBerry UEM.

Creación de una política de autenticación de Enterprise Identity

Para crear una política de Enterprise Identity para grupos de usuarios, realice la siguiente tarea.

1. En la consola de BlackBerry UEM, en la barra de menús, haga clic en **Políticas y perfiles > BlackBerry Enterprise Identity**.
2. Haga clic en **+** junto a **Políticas de autenticación**.
3. Introduzca un nombre y una descripción para el perfil.
4. En la lista desplegable **Nivel mínimo de autenticación**, especifique un nivel de autenticación. Para obtener más información, consulte [Administración de los niveles de autenticación](#).
5. En la tabla **Escenarios de riesgo**, haga clic en **+**.
6. Introduzca un nombre y una descripción.
7. En la lista desplegable **Nivel mínimo de autenticación**, seleccione el nivel de autenticación que desee aplicar cuando se cumplan los factores de riesgo.
8. En la lista **Combinación de factores de riesgo**, seleccione una de las opciones siguientes:
 - Si desea aplicar todos los factores de riesgo seleccionados al escenario, seleccione **Se dan todos los factores seleccionados**.
 - Si desea que se aplique cualquiera de los factores de riesgo seleccionados al escenario, seleccione **Se da alguno de los factores seleccionados**.
9. Si desea evaluar si una aplicación o el navegador del usuario están conectados a la misma red que el servidor de BlackBerry UEM, seleccione la opción **Detección de red**, y en la lista desplegable **Configuración**, seleccione la opción que desee. Tenga en cuenta que no podrá activar el factor de riesgo de detección de red en BlackBerry UEM Cloud.
10. Si desea establecer una referencia de confianza entre el navegador y Enterprise Identity la primera vez que abra un navegador, seleccione la opción **Detección de navegador**, y en la lista desplegable **Configuración**, seleccione la opción que desee.
11. Si desea usar los niveles de riesgo y las geozonas de BlackBerry Persona Mobile como factores de riesgo, elija la opción **BlackBerry Persona** y seleccione una de las siguientes opciones:
 - **Nivel de riesgo de comportamiento**: los servicios en la nube de BlackBerry Persona de BlackBerry Infrastructure recopilan y procesan datos de aplicaciones y los utilizan para calcular el nivel de riesgo de cada usuario.
 - **Geozona definida por el administrador**: seleccione una geozona que haya creado el administrador de BlackBerry UEM de su empresa.

Nota: Para obtener más información sobre los niveles de riesgo y las geozonas, consulte el contenido de BlackBerry Persona Mobile.
 - **Nivel de riesgo de geozona**: puede elegir Alto, Medio o Bajo. Esta configuración especifica un nivel de riesgo que puede atribuirse a un usuario al comparar la ubicación física del usuario con la región incluida en una geozona definida por el administrador o con una geozona registrada.
12. Haga clic en **Guardar**.

13. Si desea crear una excepción para cualquiera de los servicios de su empresa, haga clic en **Gestionar excepciones de servicio**, seleccione el servicio en la lista y configure cualquier escenario de riesgo necesario para el servicio.
14. Si fuera necesario, repita los pasos 5 y 11 para añadir escenarios de riesgo adicionales. Tenga en cuenta que cada escenario de riesgo debe utilizar un conjunto único de factores de riesgo.
15. Haga clic en **Guardar**.


Asignación de una política de Enterprise Identity a un grupo de usuarios

Antes de empezar: [Cree una política de Enterprise Identity](#).

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

Eliminación de una política de Enterprise Identity

Antes de empezar: [Creación de un perfil de Enterprise Identity](#).

1. En la consola de administración de BlackBerry UEM, en la barra de menús, haga clic en **Políticas y perfiles > BlackBerry Enterprise Identity**.
2. Haga clic en el nombre del perfil que desea eliminar.
3. Haga clic en  .
4. Haga clic en **Aceptar**.

Uso de la clasificación del nivel del autenticador y de las políticas de autenticación para administrar la seguridad

Puede utilizar la clasificación del nivel del autenticador y las políticas de autenticación de BlackBerry Enterprise Identity para especificar los tipos de autenticación que los usuarios deben realizar cuando inician sesión en un servicio. Las clasificaciones de autenticador son los métodos de seguridad que definen el tipo de autenticación de usuario que es necesario para iniciar sesión en un servicio. Debe utilizar escenarios de riesgo y factores de riesgo en las políticas de autenticación para especificar la configuración que se aplica a los usuarios y grupos cuando acceden a los servicios de Enterprise Identity.

Solicitud de autenticación adicional cuando los usuarios se conectan a una red externa

Lleve a cabo las siguientes tareas para solicitar a los usuarios que introduzcan su contraseña y respondan al aviso de BlackBerry 2FA cuando intenten conectarse a un servicio a través de una red externa. También puede permitir que los usuarios realicen la autenticación utilizando solo su contraseña desde cualquier red. **Nota:** No se puede activar el factor de riesgo de detección de la red en BlackBerry UEM Cloud.

Configuración de la clasificación de autenticador

1. En la barra de menú, haga clic en **Configuración > BlackBerry Enterprise Identity > Configuración**.
2. En la sección **Clasificación del nivel del autenticador**, configure **Contraseña de empresa** al nivel 1 y **Contraseña de empresa + BlackBerry 2FA** al nivel 3. Para obtener más información sobre la configuración de BlackBerry 2FA, consulte [Activación de la autenticación de dos factores](#).
3. Haga clic en **Guardar**.

Adición de una política de autenticación para redes externas

1. En la barra de menú, haga clic en **Políticas y perfiles**. Haga clic en **BlackBerry Enterprise Identity** debajo de Dispositivos gestionados.
2. En el panel **Políticas de autenticación**, haga clic en **Agregar una política**.
3. Escriba un nombre y una descripción para la política de autenticación.
4. En la lista desplegable **Nivel mínimo de autenticación**, seleccione el Nivel 1.
Este nivel se corresponde con la clasificación de autenticador de la contraseña de empresa que haya establecido en la tarea anterior. Si guarda esta política sin agregar un escenario de riesgo y la asigna a los usuarios, será necesario introducir solo la contraseña de empresa cuando se inicie sesión en un servicio. Si desea solicitar una autenticación adicional en función del tipo de red a la que se encuentre conectado, lleve a cabo los siguientes pasos para agregar un escenario de riesgo.
5. En la tabla **Escenarios de riesgo**, haga clic en +.
6. Introduzca un nombre y una descripción para el escenario.
7. En la lista desplegable **Nivel mínimo de autenticación**, seleccione el Nivel 3. Este nivel se corresponde con la clasificación de autenticador de la contraseña de empresa + BlackBerry 2FA que haya establecido en la tarea anterior.
8. Haga clic en **Detección de red**.
9. En la lista desplegable **Configuración**, seleccione **No en una red de trabajo**.

Si configura esta opción, cuando uno de los usuarios de su empresa no se encuentre en una red de trabajo e intente iniciar sesión en un servicio, deberá introducir su contraseña de empresa y responder a una solicitud en el aviso de BlackBerry 2FA en el dispositivo.

10. Haga clic en **Guardar**.

11. Haga clic en **Guardar**.

Después de terminar:

- Asigne la política de autenticación a los usuarios o grupos.

Solicitud de autenticación adicional cuando los usuarios utilizan un navegador por primera vez

Lleve a cabo las siguientes tareas para solicitar a los usuarios que introduzcan su contraseña y respondan al aviso de BlackBerry 2FA cuando intenten conectarse a un servicio utilizando un navegador por primera vez. Después de que se haya establecido la confianza, los inicios de sesión posteriores pueden usar un nivel de autenticación más simple.

Configuración de la clasificación de autenticador

1. En la barra de menú, haga clic en **Configuración > BlackBerry Enterprise Identity > Configuración**.
2. En la sección **Clasificación del nivel del autenticador**, configure **Contraseña de empresa** al nivel 1 y **Contraseña de empresa + BlackBerry 2FA** al nivel 3. Para obtener más información sobre la configuración de BlackBerry 2FA, consulte [Activación de la autenticación de dos factores](#).
3. Haga clic en **Guardar**.

Adición de una política de autenticación para la primera vez que los usuarios utilizan un navegador

1. En la barra de menú, haga clic en **Políticas y perfiles**. Haga clic en **BlackBerry Enterprise Identity** debajo de Dispositivos gestionados.
2. En el panel **Políticas de autenticación**, haga clic en **Agregar una política**.
3. Escriba un nombre y una descripción para la política de autenticación.
4. En la lista desplegable **Nivel mínimo de autenticación**, seleccione el Nivel 1.
Este nivel se corresponde con la clasificación de autenticador de la contraseña de empresa que haya establecido en la tarea anterior. Si guarda esta política sin agregar un escenario de riesgo y la asigna a los usuarios, será necesario introducir solo la contraseña de empresa cuando se inicie sesión en un servicio. Si desea solicitar datos de autenticación adicionales en el caso de que se esté utilizando el navegador por primera vez, lleve a cabo los pasos siguientes para añadir un escenario de riesgo.
5. En la tabla **Escenarios de riesgo**, haga clic en +.
6. Introduzca un nombre y una descripción para el escenario.
7. En la lista desplegable **Nivel mínimo de autenticación**, seleccione el Nivel 3. Este nivel se corresponde con la clasificación de autenticador de la contraseña de empresa + BlackBerry 2FA que haya establecido en la tarea anterior.
8. Haga clic en **Detección de red**.
9. En la lista desplegable **Configuración**, seleccione **Navegador detectado por primera vez**.
Si configura esta opción, cuando uno de los usuarios de su empresa esté utilizando un navegador por primera vez e intente iniciar sesión en un servicio, deberá introducir su contraseña de empresa y responder a una solicitud en el aviso de BlackBerry 2FA en el dispositivo.
10. Haga clic en **Guardar**.

11. Haga clic en **Guardar**.

Después de terminar:

- Asigne la política de autenticación a los usuarios o grupos.

Activación de la autenticación de los usuarios con PingFederate

BlackBerry Enterprise Identity puede redirigir la autenticación a PingFederate, que proporciona a los usuarios de Ping Identity existentes una interfaz de usuario familiar. También puede utilizar directivas de BlackBerry Enterprise Identity o BlackBerry Intelligent Security para permitir que la autenticación de Ping Identity se adapte tanto al riesgo como al contexto, incluida la extensión mediante PingID o la autenticación multifactor de BlackBerry 2FA.

Para que BlackBerry Enterprise Identity y PingFederate puedan comunicarse, debe crear un cliente de Ping Identity en el servidor PingFederate de su empresa y un proveedor de identidad correspondiente en BlackBerry UEM.

Antes de crear un cliente de Ping Identity, asegúrese de que la directiva de autenticación de PingFederate de su empresa tiene el atributo OBJECTGUID establecido en Hex. Para obtener más información, consulte la documentación de Ping Identity.

Nota: Debe tener la versión más reciente de BlackBerry UEM 12.11 instalada en su entorno.

Creación de un cliente de Ping Identity en un servidor de PingFederate

Antes de que los usuarios de BlackBerry Enterprise Identity puedan autenticarse con PingFederate, debe configurar un cliente de Ping Identity en el servidor de PingFederate de su empresa.

1. Inicie sesión en la consola de administrador de PingFederate.
2. Haga clic en **Servidor de OAuth**.
3. En la columna Clientes, haga clic en **Crear nuevo**.
4. En el campo **ID de cliente**, escriba un ID exclusivo para el cliente. Tenga en cuenta que utilizará este mismo ID cuando configure el proveedor de identidades en BlackBerry UEM.
5. Escriba un nombre y una descripción para el cliente.
6. En la sección Autenticación de cliente, haga clic en **JWT de clave privada**.
7. Seleccione la opción **Requerir solicitudes con firma**.
8. Para generar un conjunto de claves web JSON, vaya a <https://mkjwk.org/>.
9. Haga clic en la pestaña **Curva elíptica**.
10. En la lista desplegable **Curva**, seleccione **P-256**.
11. En la lista desplegable **Algoritmo** y seleccione **ES256**.
12. Haga clic en **Clave nueva**.
13. Copie la clave del campo **Conjunto de pares de claves**. Tenga en cuenta que utilizará la misma clave en la tarea [Configuración de un proveedor de identidad en BlackBerry UEM](#).
14. Pegue la clave en el campo **JWKS** del sitio PingFederate.
15. En el campo **URI de redirección**, agregue el URI del servidor de PingFederate de su empresa y haga clic en **Agregar**.
16. En la sección **Concesiones permitidas**, seleccione la opción **Código de autorización**.
17. En la lista desplegable **Algoritmo de firma de identificador de ID**, seleccione cualquiera de las opciones de **ECDSA**. Tenga en cuenta que utilizará la misma opción en la tarea [Configuración de un proveedor de identidad en BlackBerry UEM](#).
18. Haga clic en **Guardar**.

Después de terminar: [Configuración de un proveedor de identidad en BlackBerry UEM](#)

Configuración de un proveedor de identidad en BlackBerry UEM

Tras crear un cliente Ping Identity, debe crear un proveedor de identidad correspondiente en la consola de gestión de BlackBerry UEM.

Antes de empezar: [Creación de un cliente de identidad Ping en un servidor PingFederate](#)

1. En la consola de gestión de BlackBerry UEM, haga clic en **Configuración > BlackBerry Enterprise Identity > Proveedores de identidad**.
2. Haga clic en **+** y seleccione **PingFederate**.
3. En el campo **Nombre**, escriba un nombre para el proveedor de identidades.
4. En el campo **URL de documento de detección de OIDC**, escriba la ubicación del servidor de PingFederate de su empresa.
5. En el campo **ID de cliente**, introduzca el mismo ID utilizado en la sección [Creación de un cliente de identidad Ping en un servidor PingFederate](#).
6. En el campo **Clave JWKS privada**, introduzca la misma clave utilizada en la sección [Creación de un cliente de identidad Ping en un servidor PingFederate](#).
7. En la lista desplegable **Algoritmo de firma de identificador de ID**, seleccione la misma opción elegida en la sección [Creación de un cliente de identidad Ping en un servidor PingFederate](#).
8. En la lista **Servicios disponibles**, seleccione los servicios que desee asignar al cliente Ping Identity y haga clic en la flecha hacia la derecha para agregar el servicio a la lista **Servicio seleccionado**. Tenga en cuenta que solo puede asignar un cliente Ping Identity a cada servicio.
9. Haga clic en **Guardar**.

Creación de una política de BlackBerry Enterprise Identity para usuarios de PingFederate

1. En la barra de menús de la consola de BlackBerry UEM, haga clic en **Políticas y perfiles > BlackBerry Enterprise Identity > Agregar una política**.
2. Escriba un nombre y una descripción para la política.
3. En la lista desplegable **Nivel mínimo de autenticador**, seleccione el número que corresponda a uno de los niveles de autenticación de Ping Identity en la pantalla **Configuración > BlackBerry Enterprise Identity > Configuración**. Puede elegir el nivel correspondiente a las siguientes opciones: Contraseña de Ping, Contraseña de Ping + BlackBerry 2FA o Contraseña de Ping + PingID.
4. Opcionalmente, puede añadir un Escenario de riesgo que proporcione seguridad adicional si existen determinadas condiciones; por ejemplo, si un usuario no se encuentra en una red interna. En la tabla **Escenarios de riesgo**, haga clic en **+**.
5. Introduzca un nombre y una descripción para el escenario de riesgo.
6. Seleccione un Nivel mínimo de autenticación que corresponda a uno de los Niveles de autenticador de Ping en la pantalla **Configuración > BlackBerry Enterprise Identity > Configuración**. Puede optar por permitir que los usuarios introduzcan únicamente su contraseña, respondan a un aviso de BlackBerry 2FA o introduzcan su PingID si existe alguno de los factores de riesgo cuando el usuario inicia sesión en el servicio. Elija entre los siguientes factores de riesgo:
 - **Detección de red:** si desea evaluar si una aplicación o el navegador del usuario están conectados a la misma red que BlackBerry UEM, seleccione la opción **Detección de red** y, en la lista desplegable **Configuración**, seleccione la opción que desee.
 - **Detección de navegador:** si desea establecer una referencia de confianza entre el navegador y Enterprise Identity la primera vez que el usuario abra un navegador, seleccione la opción **Detección de navegador** y, en la lista desplegable **Configuración**, seleccione la opción que desee.

- **BlackBerry Persona:** si desea utilizar los niveles de riesgo y las geozonas de BlackBerry Persona Mobile como factores de riesgo, elija la opción BlackBerry Persona.

7. Haga clic en **Guardar**.

8. Haga clic en **Guardar**.

Después de terminar: Asigne la política a los usuarios de PingFederate de su empresa. Si tiene los usuarios configurados en un grupo, puede seguir el tema [Asignación de una política de Enterprise Identity a un grupo de usuarios](#) para asignar fácilmente la política a todos los usuarios a la vez.

Activación de la autenticación de los usuarios con Okta

BlackBerry Enterprise Identity puede redirigir la autenticación a Okta, que proporciona a los usuarios de Okta existentes una interfaz de usuario familiar. También puede utilizar las políticas de BlackBerry Enterprise Identity o BlackBerry Persona para permitir que la autenticación de Okta se adapte al riesgo y al contexto, incluida la autenticación multifactor de BlackBerry 2FA.

Para que BlackBerry Enterprise Identity y PingFederate puedan comunicarse, debe crear un cliente de Ping Identity en el servidor PingFederate de su empresa y un proveedor de identidad correspondiente en BlackBerry UEM.

Antes de crear un cliente de Ping Identity, asegúrese de que la directiva de autenticación de PingFederate de su empresa tiene el atributo OBJECTGUID establecido en Hex. Para obtener más información, consulte la documentación de Ping Identity.

Nota: Debe tener la versión más reciente de BlackBerry UEM 12.11 instalada en su entorno.

Creación de una aplicación Okta

Antes de empezar:

La instancia de Okta debe tener una conexión a Microsoft Active Directory y los usuarios deben importarse a Okta. Para obtener instrucciones, consulte <https://help.okta.com/en/prod/Content/Topics/Directory/ad-agent-main.htm>

1. Inicie sesión en la consola de gestión de Okta.

2. Cree un token de seguridad.

- a) Haga clic en **Seguridad > API > Tokens**.
- b) Haga clic en **Crear token**.
- c) Copie el token.

3. Genere las claves JWKS.

- a) Vaya a <https://mkjwk.org>.
- b) Haga clic en la pestaña **EC**.
- c) En la lista desplegable **Curva**, seleccione **P-521**.
- d) En la lista desplegable **Algoritmo**, seleccione **ES521: ECDSA utilizando P-521 y SHA-512**.
- e) En la lista desplegable **ID de clave**, seleccione **SHA-256**.
- f) Copie el par de claves público y privado, el conjunto de pares de claves y la clave pública.

Nota: En el conjunto de claves público y privado, debe eliminar el atributo "**d**": porque es una clave privada.

4. En un símbolo del sistema, utilice una solicitud CURL/postman para registrar una aplicación OIDC con Okta actualice los siguientes campos en JSON. La consola de Okta no admite actualmente la creación de este tipo de aplicación.

- Compruebe que el valor de SSWS de autorización es el token que creó en el paso 2.
- Sustituya las llaves jwks por las claves del paso 3.

- Compruebe que se ha eliminado el atributo "d".

Su entrada debe ser similar a la siguiente.

```
curl --request POST 'https://<oktaDomain>.okta.com/api/v1/apps/' \
--header 'Authorization: SSWS <token>' \
--header 'Content-Type: application/json' \
--data-raw '{
  "name": "oidc_client",
  "label": "BlackBerry Enterprise ID Client",
  "signOnMode": "OPENID_CONNECT",
  "credentials": {
    "oauthClient": {
      "token_endpoint_auth_method": "private_key_jwt"
    }
  },
  "settings": {
    "oauthClient": {
      "redirect_uris": [
        "https://idp.blackberry.com/idp/externalIdpCb"
      ],
      "response_types": [
        "code"
      ],
      "grant_types": [
        "authorization_code"
      ],
      "application_type": "native",
      "jwks": {
        "keys": [
          {
            "kty": "EC",
            "alg": "P-521",
            "kid": "OJE1cjnUBHGxHtOiHc64gS01xxNzhoe9sRorb2CCKgU",
            "x":
"AV4Ljfy12eCoPloyO_U3047BTprKxuw1Um57p7FsQJFMtW1Xks7j8IQe4H0S8tNpd21Q_2NcKiJg5gj
Wks0H30h6",
            "y": "AIWYPJ-
c1UWEWQX04Zk13TKCPxCiAqv7ju_vJs00Jye7zC1SzqAFbfIzCRRq_MJJJfmw2ZbfgtvHmG2
8avR10287",
            "alg": "ES512"
          }
        ]
      }
    }
  }
}'
```

Para obtener información sobre la especificación JSON, consulte <https://developer.okta.com/docs/reference/api-overview/>

5. Vea su aplicación en la consola de Okta y copie el **ID de cliente**.
6. Asigne la aplicación a los usuarios. Para obtener instrucciones, consulte <https://help.okta.com/en/prod/Content/Topics/Provisioning/lcm/lcm-user-app-assign.htm>.
7. Para configurar las notificaciones de ID de Okta, vaya a **Seguridad > API > Servidor de autorización** y seleccione su servidor de autorización.
8. En la pestaña **Notificaciones**, haga clic en **Agregar notificaciones** y agregue una notificación con los siguientes valores:
 - a) **Nombre:** object_guid

- b) **Incluir en tipo de identificador:** Identificador de token, siempre
 - c) **Tipo de valor:** Expresión
 - d) **Valor:** findDirectoryUser().externalId
9. Haga clic en **Crear**.

Configuración de Okta como un proveedor de identidad en BlackBerry UEM

Tras crear un cliente Okta, debe crear un proveedor de identidad correspondiente en la consola de gestión de BlackBerry UEM.

Antes de empezar: Creación de una aplicación Okta

1. En la consola de gestión de BlackBerry UEM, haga clic en **Configuración > BlackBerry Enterprise Identity > Proveedores de identidad**.
2. Haga clic en **+** y seleccione **Okta**.
3. En el campo **Nombre**, escriba un nombre para el proveedor de identidades.
4. En el campo **URL de documento de detección de OIDC**, escriba la ubicación del servidor de Okta de su empresa. Por ejemplo, `https://<oktaDomain>.okta.com/.well-known/oauth-authorization`
5. En el campo **Id. de cliente**, introduzca el mismo ID de cliente que creó en la tarea [Creación de una aplicación Okta](#).
6. En el campo **Clave privada JWKS**, introduzca la clave privada que utilizó en la tarea [Creación de una aplicación Okta](#).

Su entrada debe ser similar a la siguiente.

```
curl --request POST 'https://<oktaDomain>.okta.com/api/v1/apps/' \
--header 'Authorization: SSWS <token>' \
--header 'Content-Type: application/json' \
--data-raw '{
  "name": "oidc_client",
  "label": "BlackBerry Enterprise ID Client",
  "signOnMode": "OPENID_CONNECT",
  "credentials": {
    "oauthClient": {
      "token_endpoint_auth_method": "private_key_jwt"
    }
  },
  "settings": {
    "oauthClient": {
      "redirect_uris": [
        "https://idp.blackberry.com/idp/externalIdpCb"
      ],
      "response_types": [
        "code"
      ],
      "grant_types": [
        "authorization_code"
      ],
      "application_type": "native",
      "jwks": {
        "keys": [
          {
            "kty": "EC",
            "alg": "P-521",
            "kid": "OJE1cjnUBHGxHtOiHc64gS0lxxNzhoe9sRorb2CCKgU",
            "x":
"AV4Ljfy12eCoPloyO_U3047BTprKxuw1Um57p7FsQJFMtW1Xks7j8IQe4H0S8tNpd21Q_2NcKiJg5gj"
```

```
        "y": "AIWYPJ-  
c1UWEWQXO4Zkl3TKCPxCiAqv7ju_vJs00Jye7zC1SzqAFbfIzCRRq_MJJJfmw2ZbfgtvHmG2  
8avR1O287",  
        "alg": "ES512"  
    }  
  ]  
}  
}'
```

7. En la lista **Servicios disponibles**, seleccione los servicios que desea asignar al cliente Okta y haga clic en la flecha derecha para añadir el servicio a la lista **Servicio seleccionado**. Tenga en cuenta que solo puede asignar un cliente Okta a cada servicio.

8. Haga clic en **Guardar**.

Después de terminar: [Creación de una política de autenticación de Enterprise Identity](#) y asígnelo a usuarios o grupos. En la política, agregue el servicio en Gestionar excepciones de servicio y establezca el nivel de autenticación mínimo en Nivel 4.

Administración de grupos de aplicaciones

Puede usar grupos de aplicaciones para crear una colección de aplicaciones en BlackBerry UEM y asignarlas a usuarios, grupos de usuarios o grupos de dispositivos. La agrupación de aplicaciones contribuye a aumentar la eficiencia y la coherencia al administrar aplicaciones. Por ejemplo, puede utilizar grupos de aplicaciones para agrupar las mismas aplicaciones para varios tipos de dispositivos o para agrupar aplicaciones para usuarios con la misma función en la empresa. Con BlackBerry Enterprise Identity, un grupo de aplicaciones también puede contener la autorización con inicio de sesión único, además de los archivos de origen de las aplicaciones móviles para acceder a un servicio específico. Esto le permite ofrecer a los usuarios todo lo que necesitan para acceder al servicio con una única acción.

Puede utilizar la consola de administración de BlackBerry UEM para administrar los grupos de aplicaciones. Para obtener más información, consulte [Administración de grupos de aplicaciones](#), en el contenido referente a la administración de BlackBerry UEM.

Asignación de autorizaciones a usuarios o grupos

Antes de empezar: Debe agregar los usuarios y los servicios en BlackBerry UEM antes de poder conceder autorizaciones a los usuarios para que utilicen los servicios. Para obtener más información sobre la adición de servicios, consulte la guía [Integración de los servicios de SaaS](#). Tras sincronizar los servicios de Enterprise Identity con BlackBerry UEM, los servicios estarán disponibles en la consola de administración en forma de aplicaciones. Asigne una aplicación a un usuario para autorizarle a utilizar dicho servicio.

1. En la consola de administración de BlackBerry UEM, seleccione el usuario o el grupo de usuarios al que desea asignar las autorizaciones. Lleve a cabo una de las siguientes acciones:
 - Para asignar autorizaciones a un usuario, haga clic en la opción **Usuarios** de la barra de menú y seleccione su nombre.
 - Para asignar autorizaciones a un grupo, haga clic en la opción **Grupos** de la barra de menú y seleccione un grupo. Haga clic en la pestaña **Configuración**.
2. Seleccione la aplicación o el grupo de aplicaciones que desea asignar.
3. Haga clic en la casilla de verificación situada junto al servicio que desea asignar.
4. Haga clic en **Asignar**.
5. Si se le solicita que asigne las licencias, haga clic en **Sí**.

Cambio de la configuración de Enterprise Identity

Algunas opciones de BlackBerry Enterprise Identity pueden ajustarse con la consola de administración de BlackBerry UEM. Puede cambiar el nombre para mostrar de las credenciales en la página de inicio de sesión de Enterprise Identity. También puede ajustar la clasificación de los autenticadores. El proceso de autenticación de los servicios empieza en el autenticador con la clasificación más alta y continúa en orden descendiente.

1. En la barra de menús, haga clic en **Configuración > BlackBerry Enterprise Identity**.
2. Puede introducir o cambiar el nombre descriptivo de sus credenciales de BlackBerry UEM en el cuadro de texto Nombre.
3. Para cambiar la clasificación de los autenticadores, haga clic en las flechas arriba o abajo de la columna **Clasificación**. Mobile ZSO no es compatible con todos los servicios, por lo que si ese autenticador se coloca en la parte superior, algunos servicios no estarán disponibles.
4. Haga clic en **Guardar**.

Personalización de la página de inicio de sesión de usuario de su empresa

Puede personalizar la página de inicio de sesión de usuario de BlackBerry Enterprise Identity de su empresa. Por ejemplo, puede añadir el logotipo de la empresa.

1. En la consola de administración de BlackBerry UEM, en la barra de menú, haga clic en **Aplicaciones**.
2. Haga clic en **Agregar una aplicación**.
3. Haga clic en **Enterprise Identity**. Aparece un mensaje que le solicita que sincronice los servicios de Enterprise Identity.
4. Haga clic en **Abrir consola de Enterprise Identity**. La consola de administrador se abre en una nueva pestaña del navegador. Si la consola no se abre, asegúrese de que ha activado los elementos emergentes en el navegador.
5. Haga clic en **Enterprise**.
6. En el campo **Texto de seguridad de inicio de sesión**, escriba cualquier información adicional que desee que los usuarios tengan en cuenta. Este texto se mostrará debajo del campo Contraseña en la página de inicio de sesión.
7. En el campo **Título de inicio de sesión**, escriba el texto que se mostrará en la parte superior de la página de inicio de sesión de BlackBerry Enterprise Identity de su empresa. Puede utilizar la lista desplegable **Insertar identificador** para dar formato al texto del título de inicio de sesión.
8. En el campo **Descripción de nombre de usuario**, escriba el texto que se mostrará sobre el campo de texto de nombre de usuario de la página de inicio de sesión de BlackBerry Enterprise Identity de su empresa. Puede utilizar la lista desplegable **Insertar identificador** para dar formato al texto de la descripción de nombre de usuario.
9. En el campo **Descripción de contraseña**, escriba el texto que se mostrará sobre el campo de texto de contraseña de la página de inicio de sesión de BlackBerry Enterprise Identity de su empresa. Puede utilizar la lista desplegable **Insertar identificador** para dar formato al texto de la descripción de contraseña.
10. En el campo **Logotipo**, haga clic en **Elegir archivo** para buscar y añadir un logotipo a la página de inicio de sesión de BlackBerry Enterprise Identity de su empresa.
11. Elija opciones para los campos **Estilo de logotipo**, **Opción de color de texto** y **Fondo**.
12. Haga clic en **Guardar**.

Compatibilidad de SAML ECP para Microsoft Office 365

Algunos clientes de correo electrónico para dispositivos móviles, incluidas algunas versiones de BlackBerry Hub y BlackBerry Work no son compatibles con la interfaz ADAL de Microsoft cuando se utiliza con Microsoft Office 365, lo que evita que BlackBerry Enterprise Identity muestre su interfaz de inicio de sesión habitual. Para habilitar estos clientes de correo electrónico para dispositivos móviles, puede activar la compatibilidad de ECP (Enhanced Client or Proxy Profile) de Enterprise Identity para Office 365, lo que permite la autenticación basada en credenciales de texto como, por ejemplo, nombre de usuario y contraseña. Estas credenciales se suelen recopilar a través de la propia interfaz de usuario del cliente de correo electrónico. Tenga en cuenta que cuando se utiliza ECP para Office 365, las directivas de autenticación de Enterprise Identity no se aplican a los inicios de sesión basados en ECP.

Activación de la compatibilidad de ECP para Office 365

1. En la consola de administración de BlackBerry UEM, en la barra de menú, haga clic en **Aplicaciones**.
2. Haga clic en **Agregar una aplicación**.
3. Haga clic en **Enterprise Identity**.
4. Haga clic en **Abrir consola de Enterprise Identity**. La consola de administrador se abre en una nueva pestaña del navegador. Si la consola no se abre, asegúrese de que ha activado los elementos emergentes en el navegador.
5. En la página **Enterprise**, cambie la opción **Compatibilidad de ECP para Microsoft Office 365** a **Activado**.
6. Haga clic en **Guardar**.

Cómo impedir que los usuarios sean bloqueados en sus cuentas

Puede configurar BlackBerry Enterprise Identity para evitar que los usuarios, por ejemplo, usuarios de Active Directory, sean bloqueados en sus cuentas debido a un número elevado de intentos de inicio de sesión fallidos en BlackBerry Enterprise Identity.

1. En la consola de administración de BlackBerry UEM, en la barra de menú, haga clic en **Aplicaciones**.
2. Haga clic en **Agregar una aplicación**.
3. Haga clic en **Enterprise Identity**. Aparece un mensaje que le solicita que sincronice los servicios de Enterprise Identity.
4. Haga clic en **Abrir consola de Enterprise Identity**. La consola de administrador se abre en una nueva pestaña del navegador. Si la consola no se abre, asegúrese de que ha activado los elementos emergentes en el navegador.
5. Haga clic en **Enterprise**.
6. En la sección **Configuración de bloqueo de cuenta**, active la opción **Activar bloqueo de cuenta**.
7. Configure las siguientes opciones:
 - **Umbral de intentos de inicio de sesión**: establece el número de intentos fallidos antes de que la cuenta se bloquee temporalmente.
 - **Duración del inicio de sesión (minutos)**: establece el número de minutos durante los cuales la cuenta permanecerá bloqueada. Una vez superado este temporizador, la cuenta debería desbloquearse para el próximo intento de inicio de sesión.
 - **Restablecer duración (minutos)**: establece el número de minutos que deben transcurrir tras un intento de inicio de sesión fallido antes de que el contador de inicios de sesión fallidos se restablezca a 0.
8. Haga clic en **Guardar**.

Selección de inquilino y dominio

La mayoría de los usuarios inician la sesión en Enterprise Identity con un nombre de usuario y una contraseña, y especifican si el navegador es de confianza. Si un nombre de usuario existe en varios inquilinos o dominios, la primera vez que inicie sesión debe seleccionar el inquilino en una lista desplegable o introducir el dominio. Las selecciones se guardan para los inicios de sesión posteriores.

Gestión de inquilinos de BlackBerry UEM en la consola de BlackBerry Enterprise Identity

Puede utilizar la página de inquilinos de UEM en la consola de Enterprise Identity para gestionar los inquilinos de BlackBerry UEM de la empresa. Puede editar las propiedades de los inquilinos o desactivarlos. Tenga en cuenta que, si desactiva un inquilino, los usuarios de su empresa no podrán realizar la autenticación con ninguno de los servicios de Enterprise Identity que ha activado en BlackBerry UEM.

Puede editar las siguientes propiedades de los inquilinos de BlackBerry UEM.

Elemento	Descripción
Nombre para mostrar	Cambiar el nombre para mostrar del inquilino. Este nombre se muestra en el selector del inquilino de UEM en la pantalla de inicio de sesión, cuando hay un usuario en más de un inquilino de UEM.
Tipos de autenticador: AD	Active o desactive la instancia asociada de Microsoft Active Directory y cambie el nombre para mostrar de la instancia de Active Directory.
Tipos de autenticador: LDAP	Active o desactive el directorio asociado de LDAP y cambie el nombre para mostrar del directorio de LDAP.
Detección de red de trabajo	Active o desactive la detección de red. Este factor de riesgo determina si la aplicación o el navegador de un usuario están conectados a la misma red que el servidor de BlackBerry UEM.

Gestión de administradores y usuarios

Puede agregar o eliminar a los administradores y usuarios o cambiar sus derechos en la consola de administración de BlackBerry UEM. Para obtener más información sobre la gestión de los administradores y los usuarios, [consulte el contenido referente a la administración de BlackBerry UEM](#).


Si necesita volver a implementar BlackBerry UEM por cualquier motivo, primero, debe eliminar todos los usuarios que tienen derechos de Enterprise Identity de BlackBerry UEM. Si no se eliminan los usuarios antes de que se vuelva a implementar BlackBerry UEM, puede que estos aún tengan servicios asignados, pero no puedan acceder a ellos.

Creación de un administrador de Enterprise Identity personalizado

Puede utilizar las funciones de administrador para delegar tareas administrativas de BlackBerry Enterprise Identity específicas a usuarios. La función de administrador de seguridad de BlackBerry UEM tiene permisos totales para la gestión de la consola, que incluyen la creación y gestión de funciones y administradores. Al menos un administrador debe ser un administrador de seguridad. BlackBerry UEM incluye funciones preconfiguradas además de la función de administrador de seguridad. Puede editar o eliminar todas las funciones, a excepción de la función de administrador de seguridad. También puede crear funciones personalizadas.

Nota: Los nuevos administradores de BlackBerry Enterprise Identity personalizados que cree no podrán asignar autorizaciones de BlackBerry Enterprise Identity ni asignar aplicaciones y grupos de aplicaciones a usuarios o grupos de usuarios. Para obtener más información, consulte [Asignación de autorizaciones a usuarios o grupos](#) y [Administración de grupos de aplicaciones](#).

Antes de empezar:

- Debe ser un administrador de seguridad para crear una función personalizada.
1. En el menú izquierdo, haga clic en **Configuración > Administradores > Funciones**.
 2. Haga clic en .
 3. Escriba un nombre y una descripción para la función.
 4. En la sección **Políticas y perfiles**, seleccione las opciones de la política de Enterprise Identity. Las opciones son: **Ver política de autenticación de Enterprise Identity**, **Crear/Editar política de autenticación**, **Eliminar política de autenticación** y **Asignar política de autenticación a usuarios y grupos**.
 5. En la sección **Configuración**, seleccione las opciones de Enterprise Identity. Las opciones son: **Ver configuración de empresa de Enterprise Identity**, **Editar configuración de empresa de Enterprise Identity**, **Ver servicios de Enterprise Identity** y **Editar servicios de Enterprise Identity**.
 6. Haga clic en **Guardar**.
 7. Agregue la función a una cuenta de usuario o a un grupo de usuarios.

Después de terminar:

Para obtener más información sobre las funciones, consulte el [contenido de Administración de BlackBerry UEM](#).

Aviso legal

©2021 BlackBerry Limited. BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, CYLANCE y SECUSMART, entre otras, son marcas comerciales o marcas registradas de BlackBerry Limited, de sus subsidiarias o filiales, sujetas a licencia, cuyos derechos exclusivos están expresamente reservados. El resto de marcas comerciales pertenecen a sus respectivos propietarios.

Android y G Suite son marcas comerciales de Google Inc. Box que se incluye sin limitación como una marca comercial, marca de servicio o marca registrada de Box, Inc. iOS es una marca comercial de Cisco Systems, Inc. o de sus filiales en EE. UU. y otros países. iOS® se usa bajo licencia de Apple Inc. Azure, Microsoft, Active Directory, y Office 365 son marcas comerciales registradas o marcas comerciales de Microsoft Corporation en Estados Unidos y/o en otros países. Salesforce es una marca comercial de salesforce.com, inc. y se utiliza aquí con permiso. WebEx es una marca comercial de Cisco Systems, Inc. o de sus filiales en los Estados Unidos y en otros países. Workday es una marca comercial de Workday, Inc. El resto de marcas comerciales pertenecen a sus respectivos propietarios.

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

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

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

EN LA MEDIDA MÁXIMA EN QUE LO PERMITA LA LEY DE SU JURISDICCIÓN, EN NINGÚN CASO BLACKBERRY ASUMIRÁ RESPONSABILIDAD ALGUNA POR CUALQUIER TIPO DE DAÑOS RELACIONADOS CON ESTA DOCUMENTACIÓN O SU USO, O POR EL RENDIMIENTO O NO RENDIMIENTO DE CUALQUIER SOFTWARE,

HARDWARE, SERVICIO O PRODUCTOS Y SERVICIOS DE TERCEROS AQUÍ MENCIONADOS INCLUIDOS SIN NINGÚN TIPO DE LIMITACIÓN CUALQUIERA DE LOS SIGUIENTES DAÑOS: DIRECTOS, RESULTANTES, EJEMPLARES, INCIDENTALES, INDIRECTOS, ESPECIALES, PUNITIVOS O AGRAVADOS, DAÑOS POR PÉRDIDA DE BENEFICIOS O INGRESOS, IMPOSIBILIDAD DE CONSEGUIR LOS AHORROS ESPERADOS, INTERRUPTIÓN DE LA ACTIVIDAD COMERCIAL, PÉRDIDA DE INFORMACIÓN COMERCIAL, PÉRDIDA DE LA OPORTUNIDAD DE NEGOCIO O DAÑO O PÉRDIDA DE DATOS, IMPOSIBILIDAD DE TRANSMITIR O RECIBIR CUALQUIER DATO, PROBLEMAS ASOCIADOS CON CUALQUIER APLICACIÓN QUE SE UTILICE JUNTO CON PRODUCTOS Y SERVICIOS DE BLACKBERRY, COSTES DEBIDOS AL TIEMPO DE INACTIVIDAD, PÉRDIDA DE USO DE LOS PRODUCTOS Y SERVICIOS DE BLACKBERRY O PARTE DE ELLOS O DE CUALQUIER SERVICIO DE USO, COSTE DE SERVICIOS SUSTITUTIVOS, COSTES DE COBERTURA, INSTALACIONES O SERVICIOS, COSTE DEL CAPITAL O CUALQUIER OTRA PÉRDIDA MONETARIA SIMILAR, TANTO SI DICHS DAÑOS SE HAN PREVISTO COMO SI NO, Y AUNQUE SE HAYA AVISADO A BLACKBERRY DE LA POSIBILIDAD DE DICHS DAÑOS.

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

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

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

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

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

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

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

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

Publicado en Canadá