BlackBerry UEM

Correo electrónico, calendario y contactos

Administración

12.16

Contents

Configuración del correo de trabajo para dispositivos

Puede utilizar cualquiera de las siguientes opciones para permitir que los usuarios lean y envíen correos electrónicos de trabajo desde los dispositivos:

- Puede utilizar BlackBerry Work para gestionar el correo, el calendario y los contactos de los dispositivos de los usuarios. Para obtener más información acerca de cómo gestionar BlackBerry Work, consulte Gestión de las aplicaciones de BlackBerry Dynamics y la Guía de administración de BlackBerry Work.
- Puede utilizar los perfiles de correo electrónico para especificar la forma en la que los dispositivos se conectan al servidor de correo de la empresa y sincronizan los mensajes de correo, las entradas del calendario y los datos del organizador mediante Exchange ActiveSync o IBM Notes Traveler.
- También puede utilizar perfiles de correo IMAP/POP3 para especificar la forma en la que los dispositivos se conectan a los servidores de correo IMAP o POP3 y sincronizan los mensajes de correo.

Control de los dispositivos que pueden acceder a Exchange ActiveSync

Si su empresa utiliza Microsoft Exchange ActiveSync, puede evitar que los dispositivos utilicen Exchange ActiveSync a menos que se hayan agregado explícitamente a la lista de permitidos. Los dispositivos que no estén en la lista de admitidos no podrán acceder al correo de trabajo ni a los datos del organizador. El uso del BlackBerry Gatekeeping Service facilita la adición de dispositivos a la lista de permitidos. Puede utilizar BlackBerry Gatekeeping Service tanto si utiliza aplicaciones como perfiles de correo electrónico de BlackBerry Dynamics para administrar el correo, el calendario y el acceso a los contactos en los dispositivos de los usuarios.

Para utilizar BlackBerry Gatekeeping Service, debe crear una configuración de enlace de Microsoft Exchange Server o Microsoft Office 365, asignar un perfil de enlace y configurar un perfil de correo electrónico o BlackBerry Work que se dirija al servidor de enlace automático.

Cuando haya configurado BlackBerry UEM para el uso de BlackBerry Gatekeeping Service, los dispositivos del usuario se agregarán automáticamente a la lista de admitidas. Si se elimina el perfil de enlace, el perfil de correo o la aplicación de correo de un usuario, el dispositivo de dicho usuario se elimina de la lista de permitidos y deja de poder acceder a Microsoft Exchange (excepto si se le permite por otros medios, por ejemplo, Windows PowerShell).

La mayoría de dispositivos solo permiten agregar un cliente de correo electrónico a la lista de aplicaciones permitidas para cada dispositivo. Para los dispositivos Android Enterprise y Samsung Knox que utilizan una configuración de aplicación que contiene datos de marcado en lista blanca de Exchange Server, la prioridad para el marcado en lista blanca de aplicaciones de correo electrónico es la siguiente:

1. Aplicaciones de correo electrónico con configuraciones de aplicaciones que contengan datos de la lista blanca de Exchange Server
2. BlackBerry Work
3. Cliente de correo al que se envía el ID de Exchange ActiveSync durante la inscripción

Si su empresa utiliza BlackBerry UEM en un entorno local, puede instalar una o varias instancias de BlackBerry Connectivity Node para agregar instancias adicionales de los componentes de conectividad del dispositivo al dominio de su empresa. Cada BlackBerry Connectivity Node contiene una instancia de BlackBerry Gatekeeping Service. Cada instancia debe poder acceder al servidor de enlace de su empresa. Si desea que BlackBerry Gatekeeping Service, que se ha instalado con los componentes principales de BlackBerry UEM, administre los datos de enlace, puede cambiar la configuración predeterminada para desactivar BlackBerry Gatekeeping Service en cada BlackBerry Connectivity Node. Para obtener más información sobre la instalación y la configuración de BlackBerry Connectivity Node, consulte los datos del contenido de Planificación y el contenido de Instalación y actualización.

Si su empresa utiliza BlackBerry UEM Cloud, puede instalar una o varias instancias de BlackBerry Connectivity Node para agregar instancias adicionales de los componentes de conectividad del dispositivo al dominio de su empresa. Cada BlackBerry Connectivity Node contiene una instancia de BlackBerry Gatekeeping Service. Cada instancia debe poder acceder al servidor de Exchange ActiveSync de su empresa. Si desea gestionar la configuración de acceso de Exchange ActiveSync solo mediante el BlackBerry Gatekeeping Service que se ha instalado con BlackBerry Connectivity Node principal, cambie la configuración predeterminada para desactivar BlackBerry Gatekeeping Service en las instancias de BlackBerry Connectivity Node adicionales. Para obtener más información sobre la instalación y configuración de un BlackBerry Connectivity Node, consulte Instalación o actualización de BlackBerry Connectivity Node en el contenido de configuración de BlackBerry UEM Cloud.

Puede configurar grupos de servidores para dirigir el tráfico de conectividad de dispositivos a una conexión regional específica a BlackBerry Infrastructure. Al asociar un perfil de enlace a un grupo de servidores, cualquier usuario que tenga asignado este perfil de enlace utiliza cualquier instancia activa de BlackBerry Gatekeeping Service en ese grupo de servidores. Al configurar un grupo de servidores, puede optar por desactivar las instancias de BlackBerry Gatekeeping Service en el grupo.

Pasos para configurar Exchange ActiveSync y BlackBerry Gatekeeping Service

Cuando configura BlackBerry Gatekeeping Service, realice las acciones siguientes:

Paso	Acción
1	Configure los permisos para establecer el enlace.
2	Permita que solo los dispositivos autorizados accedan a Exchange ActiveSync.
3	Configuración de los permisos de Microsoft IIS para el enlace.
4	Cree la configuración del enlace.
5	Cree un perfil de enlace y asígnelo a cuentas de usuarios, grupos de usuarios o grupos de dispositivos.

Configure los permisos para establecer el enlace

Para utilizar el enlace de Exchange ActiveSync, debe crear una cuenta de usuario en Microsoft Exchange Server o Microsoft Office 365 y proporcionarle los permisos necesarios para establecer el enlace.

Si utiliza Microsoft Office 365, cree una cuenta de usuario de Microsoft Office 365 y asígnele las funciones de destinatarios de correo y acceso de clientes de la empresa.

Si utiliza Microsoft Exchange Server, siga las instrucciones a continuación para configurar funciones de administración con los permisos correctos para gestionar los buzones de correo y el acceso de los clientes de Exchange ActiveSync. Para realizar esta tarea, debe ser un administrador de Microsoft Exchange con los permisos adecuados para crear y cambiar las funciones de administración.

Antes de empezar:

- En el equipo que aloja Microsoft Exchange, cree una cuenta y un buzón de correo para gestionar enlaces en BlackBerry UEM (por ejemplo, BUEMAdmin). Al crear una configuración de Exchange ActiveSync debe especificar la información de inicio de sesión para esta cuenta. Anote el nombre de esta cuenta, ya que deberá indicarlo al final de la tarea que aparece a continuación.
- WinRM debe estar configurado con la configuración predeterminada en el equipo que aloja el Microsoft Exchange Server que se configura para establecer el enlace. Debe ejecutar el comando `Winrm quickconfig` en un símbolo del sistema como un administrador. Cuando la herramienta muestre `Make these changes [y/n]`, escriba `y`. Una vez que el comando se haya ejecutado correctamente, verá el siguiente mensaje.

```
WinRM se actualizó para administración remota.


Se cambió el tipo de servicio WinRM a inicio automático retrasado,

Servicio WinRM iniciado.
```

```
Se creó una escucha WinRM en HTTP://* para aceptar solicitudes de WS-Man en

 cualquier IP de este equipo.
```

1. Abra Microsoft Exchange Management Shell.
2. Escriba `New-ManagementRole -Name "<name_new_role_mail_recipients>" -Parent "Mail Recipients"`. Pulse INTRO.
3. Escriba `New-ManagementRole -Name "<name_new_role_org_ca>" -Parent "Organization Client Access"`. Pulse INTRO.
4. Escriba `New-ManagementRole -Name "<name_new_role_exchange_servers>" -Parent "Exchange Servers"`. Pulse INTRO.
5. Escriba `Get-ManagementRoleEntry "<name_new_role_mail_recipients>\*" | Where {$_.Name -ne "Get-ADServerSettings"} | Remove-ManagementRoleEntry`. Pulse INTRO.
6. Escriba `Get-ManagementRoleEntry "<name_new_role_org_ca>\*" | Where {$_.Name -ne "Get-CasMailbox"} | Remove-ManagementRoleEntry`. Pulse INTRO.
7. Escriba `Get-ManagementRoleEntry "<name_new_role_exchange_servers>\*" | Where {$_.Name -ne "Get-ExchangeServer"} | Remove-ManagementRoleEntry`. Pulse INTRO.
8. Escriba `Add-ManagementRoleEntry "<name_new_role_mail_recipients>\Get-ActiveSyncDeviceStatistics" -Parameters Mailbox`. Pulse INTRO.
9. Escriba `Add-ManagementRoleEntry "<name_new_role_mail_recipients>\Get-ActiveSyncDevice" -Parameters Identity`. Pulse INTRO.
10. Escriba `Add-ManagementRoleEntry “<name_new_role_mail_recipients>\Get-MobileDeviceStatistics” –Parameters Mailbox`. Pulse INTRO.
11. Escriba `Add-ManagementRoleEntry “<name_new_role_mail_recipients>\Get-MobileDevice” –Parameters Mailbox`. Pulse INTRO.
12. Escriba `Add-ManagementRoleEntry "<name_new_role_org_ca>\Set-CasMailbox" -Parameters Identity, ActiveSyncBlockedDeviceIDs, ActiveSyncAllowedDeviceIDs`. Pulse INTRO.
13. Escriba `New-RoleGroup "<name_new_group>" -Roles "<name_new_role_mail_recipients>", "<name_new_role_org_ca>", "<name_new_role_exchange_servers>"`. Pulse INTRO.
14. Escriba `Add-RoleGroupMember -Identity "<name_new_group>" -Member "BUEMAdmin"`. Pulse INTRO.
15. Escriba `Add-Management RoleEntry " <name_new_role_mail_recipients>\ Set-Ad ServerSettings" .` Pulse INTRO.
16. Escriba `Add-ManagementRoleEntry "<name_new_role_mail_recipients>\Remove-ActiveSyncDevice" -Parameters Identity,Confirm`. Pulse INTRO.
17. Escriba `Add-ManagementRoleEntry "<name_new_role_mail_recipients>\Remove-MobileDevice" -Parameters Identity,Confirm`. Pulse INTRO.

Después de terminar: Permita que solo los dispositivos autorizados accedan a Exchange ActiveSync.

Permita que solo los dispositivos autorizados accedan a Exchange ActiveSync

Si su empresa utiliza Microsoft Exchange Server, consulte Configuración de Microsoft Exchange para permitir que solo los dispositivos autorizados accedan a Exchange ActiveSync.

Si su empresa utiliza Microsoft Office 365, consulte Configuración de la política de acceso con dispositivos móviles de Microsoft Office 365.

Configuración de Microsoft Exchange para permitir que solo los dispositivos autorizados accedan a Exchange ActiveSync

Debe configurar Microsoft Exchange Server para permitir que solo los dispositivos autorizados accedan a Exchange ActiveSync. Los dispositivos para los usuarios que no se agregan explícitamente a la lista de permitidos en Microsoft Exchange deben estar en cuarentena hasta que BlackBerry UEM les permita el acceso.

Solo puede enumerarse en la lista blanca un correo electrónico de cliente por dispositivo. La prioridad para la aplicación de la lista blanca de correos electrónicos sería la siguiente:

1. Aplicaciones de correo electrónico cuya configuración incluya datos de la lista blanca de Exchange Server (solo para Android Enterprise o Samsung KNOX Play for Work)
2. BlackBerry Work
3. Cliente de correo al que se envía el ID de EAS durante la inscripción

Para realizar esta tarea, debe ser un administrador de Microsoft Exchange con los permisos adecuados para configurar Set-ActiveSyncOrganizationSettings. Para obtener más información acerca de cómo permitir que solo los dispositivos autorizados accedan a Exchange ActiveSync, visite https://technet.microsoft.com y lea el artículo *Activar un dispositivo para Exchange ActiveSync*.

Antes de empezar:

- Configure los permisos para establecer el enlace.
- Verifique con el administrador de Microsoft Exchange si hay o no hay usuarios utilizando actualmente Exchange ActiveSync.
- Si el nivel de acceso predeterminado para Exchange ActiveSync de la empresa se configura como "permitir" y los usuarios configuran y sincronizan correctamente sus dispositivos, debe asegurarse de que estos usuarios tengan una exención personal o una regla de dispositivo asociada a la cuenta de usuario o dispositivo antes de establecer el nivel de acceso predeterminado en cuarentena. Si no lo hacen, se ponen en cuarentena y los dispositivos no se sincronizarán hasta que BlackBerry UEM los permita. Para obtener más información sobre cómo configurar el nivel de acceso predeterminado para Exchange ActiveSync en cuarentena, visite support.blackberry.com/community y lea el artículo 36800.

1. En un ordenador que aloje Microsoft Exchange Management Shell, abra Microsoft Exchange Management Shell.
2. Escriba `Set-ActiveSyncOrganizationSettings –DefaultAccessLevel Quarantine`. Pulse INTRO.

Después de terminar: Configuración de los permisos de Microsoft IIS para el enlace.

Configuración de la política de acceso con dispositivos móviles de Microsoft Office 365

Para utilizar BlackBerry Gatekeeping Service con Microsoft Office 365, debe configurar la política de acceso con dispositivos móviles en Microsoft Office 365 para poner en cuarentena los dispositivos de forma predeterminada.

Antes de empezar:

- Configure los permisos para establecer el enlace.
- Si el nivel de acceso predeterminado para Exchange ActiveSync de la empresa se configura como "permitir" y los usuarios configuran y sincronizan correctamente sus dispositivos, debe asegurarse de que estos usuarios tengan una exención personal o una regla de dispositivo asociada a la cuenta de usuario o dispositivo antes de establecer el nivel de acceso predeterminado en cuarentena. Si no lo hacen, se ponen en cuarentena y los dispositivos no se sincronizarán hasta que BlackBerry UEM. Para obtener más información acerca de cómo establecer el nivel de acceso predeterminado para Exchange ActiveSync en cuarentena, visite support.blackberry.com/community y lea el artículo 33531.

1. Inicie sesión en el portal de administración de Microsoft Office 365.
2. En el menú lateral, haga clic en **Administrar**.
3. Haga clic en **Exchange**.

4. En la sección **Móvil**, haga clic en **acceso con dispositivo móvil**.
5. Haga clic en **Editar**.
6. Haga clic en **Cuarentena: dejarme decidir si deseo bloquear o permitir más tarde**.

Después de terminar: Configuración de los permisos de Microsoft IIS para el enlace.

Configuración de los permisos de Microsoft IIS para el enlace

BlackBerry UEM utiliza comandos de Windows PowerShell para gestionar la lista de dispositivos permitidos. Para utilizar BlackBerry Gatekeeping Service, debe configurar los permisos de Microsoft IIS. Realice las siguientes acciones en el equipo que aloja la función de servidor de acceso de cliente de Microsoft.

Antes de empezar: Permita que solo los dispositivos autorizados accedan a Exchange ActiveSync.

1. Abra el Administrador de Microsoft Internet Information Services (IIS).
2. En el panel izquierdo, expanda el servidor.
3. Expanda **Sitios** > **Sitio web predeterminado**.
4. Haga clic con el botón derecho en la carpeta PowerShell. Seleccione **Editar permisos**.
5. Haga clic en la pestaña **Seguridad**. Haga clic en **Editar**.
6. Haga clic en **Agregar** e introduzca el <nuevo_grupo> que se creó cuando se configuraron los permisos de Microsoft Exchange para el enlace.
7. Haga clic en **Aceptar**.
8. Confirme que las opciones **Leer y ejecutar**, **Enumerar contenido de carpetas** y **Leer** están seleccionadas. Haga clic en **Aceptar**.
9. Seleccione la carpeta **PowerShell**. Haga doble clic en el icono **Autenticación**.
10. Seleccione **Autenticación de Windows**. Haga clic en **Activar**.
11. Cierre el Administrador de Microsoft Internet Information Services (IIS).

Después de terminar: Cree la configuración del enlace.

Agregar una aplicación y obtener los detalles de Azure para configurar la autenticación moderna

Cuando esté configurando la autenticación moderna, deberá proporcionar dos detalles de la aplicación: ID de la aplicación y empresa.

1. Inicie sesión en portal.azure.com.
2. Haga clic en **App registrations**.
3. Haga clic en **Nuevo registro**.
4. En el campo **Nombre**, escriba un nombre para la aplicación.
5. Haga clic en **Registrar**.
6. Haga clic en **Permisos de API > Agregar un permiso**.
7. Busque el grupo de permisos **Exchange** o **Office 365 Exchange Online**.
8. Haga clic en **Permisos de aplicaciones > Exchange.ManageAsApp > Agregar un permiso**.
9. Para otorgar el consentimiento del administrador, seleccione **Exchange.ManageAsApp > Conceder consentimiento de administrador**.

10. En la sección Administrar, haga clic en **Certificados y secretos > Cargar certificado** y seleccione la clave pública (cert.pem)
11. Para asignar una función a la aplicación, en la página de inicio de Azure, haga clic en **Azure Active Directory**.
12. Haga clic en **Funciones y administradores**.
13. En la sección **Funciones administrativas**, escriba "Exchange" para ver las funciones admitidas para Microsoft Exchange.
14. Haga clic en una función para ver los detalles de la función.
15. Haga clic en **Agregar asignaciones**.
16. En **Seleccionar miembro(s)**, haga clic en **No se ha seleccionado ningún miembro**.
17. Busque el ID de la aplicación Azure por ID de la aplicación o nombre de la aplicación.
18. Seleccione la aplicación que creó anteriormente para trasladarla a la sección **Elementos seleccionados**.
19. Haga clic en **Seleccionar**.

    El ID de la aplicación Azure ahora se muestra en la sección **Seleccionar miembros**. La información de la organización de Azure aparece en la página Azure Active Directory como una propiedad del directorio. Registre estas dos entradas para utilizarlas cuando configure BlackBerry UEM en autenticación moderna.
20. Haga clic en **Siguiente**.
21. En la página **Agregar asignaciones**, asegúrese de que el **Tipo de asignación** esté configurado en **Activo**. Para obtener más información sobre los tipos de asignación, consulte la Información de Microsoft.
22. Haga clic en **Asignar**.

Después de terminar: Cree la configuración del enlace

Asociar un certificado con el ID de aplicación de Azure para UEM

Puede solicitar y exportar un nuevo certificado de cliente desde su servidor de CA o utilizar un certificado autofirmado. La clave privada debe tener formato .pfx. La clave pública se puede exportar como un archivo .cer o .pem para cargar a Microsoft Azure.

1. Complete una de las tareas siguientes:

Certificado	Tarea
Si está utilizando un servidor CA existente	**a.** Solicite el certificado. El certificado que solicite debe incluir el nombre de la aplicación en el asunto del certificado. <*app name*> es el nombre que asignó a la aplicación en el paso 4 de Agregar una aplicación y obtener los detalles de Azure para configurar la autenticación moderna **b.** Exporte la clave pública del certificado como un archivo .cer o .pem. La clave pública se utiliza para el ID de la aplicación Azure que se crea. **c.** Exporte la clave privada del certificado como un archivo .pfx.

Si está utilizando un certificado autofirmado	**a.** Cree un certificado autofirmado con el comando New-SelfSignedCertificate. Para obtener más información, visite docs.microsoft.com y consulte New-SelfSignedCertificate. **1.** En un equipo que ejecute Microsoft Windows, abra Windows PowerShell. **2.** Introduzca el siguiente comando: `$cert=New-SelfSignedCertificate -Subject "CN=<nombre de la aplicación>" -CertStoreLocation "Cert:\CurrentUser\My" -KeyExportPolicy Exportable -KeySpec Signature`. <*app name*> es el nombre que asignó a la aplicación en el paso 4 de Agregar una aplicación y obtener los detalles de Azure para configurar la autenticación moderna El certificado que solicite debe incluir el nombre de la aplicación Azure en el campo Asunto. **3.** Pulse **Intro**. **b.** Exporte la clave pública desde la consola de administración de Microsoft (MMC). Asegúrese de guardar el certificado público como archivo .cer o .pem. La clave pública se utiliza para el ID de la aplicación Azure que se crea. **1.** En un equipo con Windows, abra el Administrador de certificados para el usuario conectado. **2.** Expanda **Personal**. **3.** Haga clic en **Certificados**. **4.** Haga clic con el botón derecho en <*usuario*>@<*dominio*> y seleccione **Todas las tareas > Exportar**. **5.** En el **Asistente para exportar certificados**, haga clic en **No exportar la clave privada**. **6.** Haga clic en **Siguiente**. **7.** Seleccione **Base-64 encoded X.509 (.cer)**. Haga clic en **Siguiente**. **8.** Ponga un nombre al certificado y guárdelo en el escritorio. **9.** Haga clic en **Siguiente**. **10.** Haga clic en **Finalizar**. **11.** Haga clic en **Aceptar**. **c.** Exporte la clave privada desde la consola de administración de Microsoft (MMC). Asegúrese de incluir la clave privada y guardarla como un archivo .pfx. Para obtener instrucciones, visite docs.microsoft.com y consulte Exportar un certificado con la clave privada. **1.** En un equipo con Windows, abra el Administrador de certificados para el usuario conectado. **2.** Expanda **Personal**. **3.** Haga clic en **Certificados**. **4.** Haga clic con el botón derecho en <*usuario*>@<*dominio*> y seleccione **Todas las tareas > Exportar**. **5.** En el **Asistente para exportar certificados**, haga clic en **Sí, exportar la clave privada**. **6.** Haga clic en **Siguiente**. **7.** Seleccione **Intercambio de información personal - PKCS # 12 (.pfx)**. Haga clic en **Siguiente**. **8.** Seleccione el método de seguridad. **9.** Ponga un nombre al certificado y guárdelo en el escritorio. **10.** Haga clic en **Siguiente**. **11.** Haga clic en **Finalizar**. **12.** Haga clic en **Aceptar**.

2. Cargue el certificado público (archivo .pem o .cer) que exportó en el paso 1 para asociar las credenciales de certificado con el ID de la aplicación Azure para UEM.
   a) En portal.azure.com, abra el <*app name*> que asignó a la aplicación en el paso 4 de Agregar una aplicación y obtener los detalles de Azure para configurar la autenticación moderna
   b) Haga clic en **Certificados y secretos**.
   c) En la sección **Certificados**, haga clic en **Cargar certificado**.
   d) En el campo de búsqueda **Seleccionar un archivo**, vaya a la ubicación donde exportó el certificado.
   e) Haga clic en **Agregar**.

Cree la configuración del enlace

Puede crear una configuración de enlace de forma que los dispositivos que cumplan con las políticas de seguridad de la empresa puedan conectarse a Microsoft Exchange Server o Microsoft Office 365.

Antes de empezar:

- Configure los permisos para establecer el enlace.
- Permita que solo los dispositivos autorizados accedan a Exchange ActiveSync.
- Configuración de los permisos de Microsoft IIS para el enlace.
- Agregue una aplicación y obtenga los detalles de Azure para configurar la autenticación moderna.

1. Lleve a cabo una de las siguientes acciones:
   - Si tiene BlackBerry UEM en un entorno local, en la barra de menú haga clic en **Configuración > Integración externa > Enlace de Microsoft Exchange**.
   - Si tiene BlackBerry UEM Cloud, en la consola de BlackBerry Connectivity Node (http:/localhost:8088) haga clic en **Configuración general > BlackBerry Gatekeeping Service**.
2. En la sección Lista de Microsoft Exchange Server, haga clic en +.
3. Lleve a cabo una de las tareas siguientes:

Tarea	Pasos
Conéctese a Microsoft Office 365 mediante la autenticación moderna	Antes de configurar BlackBerry UEM para utilizar la autenticación moderna, debe generar un certificado que tenga claves públicas y privadas. Debe utilizar OpenSSL o PowerShell para generar el certificado. **a.** Seleccione la casilla de verificación **Autenticación moderna**. **b.** En el campo **Nombre de la conexión de Exchange Online**, escriba un nombre para la conexión. **c.** Haga clic en **Examinar** y seleccione el certificado que se utilizará para la autenticación. **d.** En el campo **Contraseña del certificado**, escriba la contraseña del certificado. **e.** Especifique su **ID de la aplicación de Azure**. **f.** Especifique su **organización de Azure**.

Tarea	Pasos
Conéctese a su Microsoft Exchange Server o a Microsoft Office 365 mediante la autenticación básica	**a.** En el campo **Nombre del servidor**, escriba el nombre del entorno de Microsoft Exchange Server o Microsoft Office 365 cuyo acceso desea gestionar. **b.** Escriba el nombre de usuario y la contraseña de la cuenta que ha creado para administrar el enlace de Exchange ActiveSync. **c.** En la lista desplegable **Tipo de autenticación**, seleccione el tipo de autenticación que se utiliza en Microsoft Exchange Server o Microsoft Office 365. **d.** En la lista desplegable **Tipo de autenticación**, seleccione el tipo de autenticación que se utiliza en Microsoft Exchange Server o Microsoft Office 365. **e.** Para activar la autenticación SSL entre BlackBerry UEM y Microsoft Exchange Server o Microsoft Office 365, seleccione la casilla para marcar **Utilizar SSL**. De forma opcional, seleccione comprobaciones de certificado adicionales. **f.** En la lista desplegable **Tipo de proxy**, seleccione el tipo de configuración de proxy, si la hubiera, que se utiliza entre BlackBerry UEM y Microsoft Exchange Server o Microsoft Office 365. **g.** Si ha seleccionado una configuración proxy en el paso anterior, seleccione el tipo de autenticación que se utiliza en el servidor proxy. **h.** Si es necesario, seleccione **Autenticación requerida** y escriba el nombre de usuario y contraseña.

4. Haga clic en **Probar conexión** para comprobar que la conexión ha sido correcta.
5. Haga clic en **Guardar**.

Después de terminar:

- Creación de un perfil de enlace y asigne el perfil a las cuentas de usuario, a los grupos de usuarios o a los grupos de dispositivos.
- Si ha configurado un grupo de servidores con una o más instancias activas de BlackBerry Gatekeeping Service, asocie el perfil de enlace al grupo de servidores adecuado. Cualquier usuario que tenga este perfil de enlace asignado puede utilizar cualquier instancia activa de BlackBerry Gatekeeping Service en ese grupo de servidores.

Creación de un perfil de enlace

Si utiliza un enlace automático, cree un perfil de enlace.

Si ha configurado BlackBerry Gatekeeping Service, debe crear un perfil de enlace y asignarlo a cuentas de usuarios, grupos de usuarios o grupos de dispositivos. El perfil de enlace permite seleccionar los servidores de Microsoft Exchange para el enlace automático.

1. En la barra de menú, haga clic en **Políticas y perfiles**.
2. Haga clic en **Correo, Calendario y contactos > Enlace**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil.
5. Haga clic en **Seleccionar servidores**.
6. Seleccione uno o más servidores y haga clic en →.

7. Haga clic en **Guardar**.

Comprobación para permitir que un dispositivo tenga acceso al correo de trabajo y a los datos del organizador

Si la empresa utiliza BlackBerry Gatekeeping Service para controlar los dispositivos que pueden acceder al correo de trabajo y a los datos del organizador desde Exchange ActiveSync, al menos un servidor de enlace deberá estar configurado en un perfil de correo. Si el perfil de correo con enlace configurado está asignado a una cuenta de usuario, podrá comprobar el estado de la conexión entre un dispositivo y Exchange ActiveSync. Puede ubicar dicho estado si consulta la página de detalles del dispositivo, en la sección de política de TI y perfiles. Los estados siguientes se muestran en los detalles del dispositivo al lado del perfil de correo.

Estado	Descripción
Desconocido	Aparecerá el estado de desconocido si BlackBerry UEM no puede determinar el ID del dispositivo. El dispositivo aparecerá en la lista de dispositivos restringidos y deberá agregarse manualmente a la lista de permitidos.
Conexión pendiente	Se mostrará un estado de conexión pendiente si BlackBerry UEM conoce el ID del dispositivo y este se ha puesto en cola y está a la espera de agregarse a la lista de permitidos.
Conexión permitida	Se mostrará un estado de conexión permitida si BlackBerry UEM conoce el ID del dispositivo y este se encuentra en la lista de permitidos.

Comprobación de que el dispositivo puede acceder a Exchange ActiveSync

1. En la barra de menú, haga clic en **Usuarios > Dispositivos gestionados**.
2. Busque una cuenta de usuario.
3. En los resultados de la búsqueda, haga clic en el nombre de una cuenta de usuario.
4. Seleccione la pestaña del dispositivo que desea comprobar.
5. En la sección **Política de TI y perfiles**, si el dispositivo está permitido, se mostrará **Conexión permitida** al lado del perfil de correo.

Permitir que un dispositivo tenga acceso a Microsoft ActiveSync

Si BlackBerry UEM no puede obtener un ID de Exchange ActiveSync de un dispositivo, no se agregará a la lista de permitidos de Microsoft Exchange. Puede agregar manualmente estos dispositivos a la lista de permitidos desde la lista de dispositivos restringidos de Exchange ActiveSync. Por ejemplo, si un dispositivo con Android se activa con el tipo de activación de MDM, BlackBerry UEM no podrá obtener un ID de Exchange ActiveSync y deberá introducir manualmente el dispositivo en la lista de dispositivos restringidos de Exchange ActiveSync.

1. En la barra de menú, haga clic en **Usuarios > Enlace de Exchange**.
2. Busque un dispositivo.
3. En la columna **Acción**, haga clic en ✓.

Bloqueo de un dispositivo para que no acceda a Microsoft ActiveSync

Puede bloquear manualmente un dispositivo permitido previamente para que no acceda a Microsoft ActiveSync. El bloqueo de un dispositivo evita que un usuario recupere mensajes de correo y demás información de Microsoft Exchange Server del dispositivo.

1. En la barra de menú, haga clic en **Usuarios**.
2. Haga clic en **Enlace de Exchange**.
3. Busque un dispositivo.
4. En la columna **Acción**, haga clic en .

Creación de perfiles de correo electrónico

Puede utilizar los perfiles de correo electrónico para especificar cómo se conectan los dispositivos al servidor de correo de la empresa y cómo sincronizan los mensajes de correo, las entradas del calendario y los datos del organizador mediante Exchange ActiveSync o IBM Notes Traveler.

No es necesario utilizar un perfil de correo electrónico si su empresa utiliza BlackBerry Work para gestionar el correo electrónico, el calendario y los contactos de los dispositivos de los usuarios. Para obtener más información acerca de cómo gestionar BlackBerry Work, consulte Gestión de las aplicaciones de BlackBerry Dynamics y Guía de administración de BlackBerry Work.

Si desea utilizar Exchange ActiveSync, debe tener en cuenta lo siguiente:

- Para ampliar la seguridad de correo, puede activar S/MIME para dispositivos con iOS y dispositivos con Android.
- Si activa S/MIME, puede utilizar otros perfiles para permitir que los dispositivos puedan recuperar automáticamente los certificados S/MIME y comprobar el estado del certificado.

Si desea utilizar Notes Traveler, debe tener en cuenta lo siguiente:

- Para utilizar Notes Traveler con dispositivos iOS, debe activar BlackBerry Secure Gateway.

También puede utilizar perfiles de correo IMAP/POP3 para especificar cómo desea que los dispositivos con iOS, macOS, Android y Windows se conecten a los servidores de correo IMAP o POP3 y sincronicen los mensajes de correo. Los dispositivos activados para utilizar Knox MDM no admiten IMAP ni POP3.

Crear un perfil de correo electrónico

La configuración del perfil obligatorio varía para cada tipo de dispositivo y depende del servidor de correo utilizado en el entorno de la empresa.

Antes de empezar:

- Si utiliza autenticación basada en certificados entre los dispositivos y el servidor de correo, debe crear un perfil de certificado de CA y asignarlo a los usuarios. También se debe asegurar de que los dispositivos tengan un certificado de cliente de confianza.
- Para dispositivos Android con activaciones Controles de MDM, BlackBerry UEM envía el perfil de correo a los dispositivos , pero el usuario debe configurar manualmente la conexión con el servidor de correo.

1. En la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Correo, Calendario y contactos > Correo**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil.
5. Si fuera necesario, escriba el nombre de dominio del servidor de correo. Si el perfil es para varios usuarios que pueden estar en diferentes dominios de Microsoft Active Directory, puede utilizar la variable `%UserDomain%`.
6. En el campo **Dirección de correo electrónico**, realice una de las siguientes acciones:
   - Si el perfil es para un usuario, escriba la dirección de correo del usuario.
   - Si el perfil es para varios usuarios, escriba `%UserEmailAddress%`.
7. Escriba el nombre de host o la dirección IP del servidor de correo.
8. En el campo **Nombre de usuario**, realice una de las siguientes acciones:
   - Si el perfil es para un usuario, escriba el nombre de usuario.
   - Si el perfil es para varios usuarios, escriba `%UserName%`.

- Si el perfil es para varios usuarios en un entorno de IBM Notes Traveler, escriba `%UserDisplayName%`.

9. Si ha configurado grupos de servidores para dirigir el tráfico de BlackBerry Secure Gateway a una conexión regional determinada de BlackBerry Infrastructure, en la lista desplegable **Grupo de servidores de BlackBerry Secure Gateway Service**, haga clic en el grupo de servidores adecuado.

   Para obtener más información sobre el BlackBerry Connectivity Node y los grupos de servidores, consulte el contenido de Planificación local y el contenido de Instalación y actualización o el contenido de Configuración de UEM Cloud.
10. Haga clic en la pestaña de cada tipo de dispositivo de la empresa y configure los valores apropiados para cada configuración de perfil.
11. Haga clic en **Agregar**.

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

Configuración del perfil de correo electrónico

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

- iOS
- macOS
- Android
- Windows

Común: Configuración del perfil de correo electrónico

Común: Configuración del perfil de correo electrónico	Descripción
Nombre de dominio	Esta configuración especifica el nombre del dominio del servidor de correo.
Dirección de correo	Esta configuración especifica la dirección de correo del usuario. Si el perfil es para varios usuarios, puede utilizar la variable %UserEmailAddress%.
Nombre de host o dirección IP	Esta configuración especifica el nombre de host o la dirección IP del servidor de correo.
Nombre de usuario	Esta configuración especifica el nombre de usuario del usuario. Si el perfil es para varios usuarios, puede utilizar la variable %UserName%.
Servidores de enlace automáticos	Si ha configurado grupos de servidores para dirigir el tráfico de BlackBerry Secure Gateway o el tráfico de BlackBerry Gatekeeping Service hacia una conexión regional específica en la BlackBerry Infrastructure, esta opción especifica el grupo de servidores adecuado. Para obtener más información acerca de BlackBerry Connectivity Node y los grupos de servidores en un entorno local, consulte el contenido de Planificación y el contenido de Instalación y actualización. Para obtener más información sobre BlackBerry Connectivity Node y los grupos de servidores en un entorno en la nube, consulte el contenido de Configuración de BlackBerry UEM Cloud.

iOS: configuración del perfil de correo

Esta configuración se aplica también a dispositivos con iPadOS.

iOS: configuración del perfil de correo	Descripción
Configuración de entrega	
Permitir que los mensajes se muevan	En la configuración se especifica si desea que los usuarios puedan mover mensajes de correo desde esta cuenta a otra cuenta de correo en un dispositivo.
Permitir la sincronización de direcciones recientes	En la configuración se especifica si un usuario puede sincronizar direcciones utilizadas recientemente a través de los dispositivos.
Utilizar solo con correo	En la configuración se especifica si desea que las aplicaciones que no sean la aplicación de correo puedan utilizar esta cuenta para enviar mensajes de correo.
Activar S/MIME	Esta configuración especifica si un usuario puede enviar mensajes de correo protegidos con S/MIME.
Activar mensajes de S/MIME con firma digital	En la configuración se especifica si desea que un dispositivo envíe mensajes de salida con una firma digital. Esta configuración es válida únicamente si se ha seleccionado la opción "Activar S/MIME".
Credenciales de firma	En la configuración se especifica cómo los dispositivos encuentran los certificados necesarios para firmar los mensajes. Esta configuración es válida únicamente si se ha seleccionado la opción "Activar S/MIME". Valores posibles: • Certificado compartido • SCEP • Credencial de usuario Después de elegir el tipo de perfil que desea utilizar, puede especificar el certificado compartido, el SCEP o el perfil de credenciales de usuario. Esta configuración es válida únicamente si se ha seleccionado la opción "Activar S/MIME".
Certificado compartido de firma	Esta configuración especifica el perfil de certificado compartido para un certificado de cliente que un dispositivo utiliza para firmar mensajes de correo. Esta configuración es válida únicamente si se ha seleccionado la opción "Activar S/MIME".
SCEP de firma	Esta configuración especifica el perfil SCEP que los dispositivos pueden utilizar para recuperar los certificados necesarios para firmar mensajes de correo mediante S/MIME. Esta configuración es válida únicamente si se ha seleccionado la opción "Activar S/MIME".

iOS: configuración del perfil de correo	Descripción
Credenciales de usuario de firma	Esta configuración especifica el perfil de credenciales de usuario que los dispositivos pueden utilizar para obtener los certificados de clientes necesarios para firmar mensajes de correo mediante S/MIME. Esta configuración es válida únicamente si se ha seleccionado la opción "Activar S/MIME".
El usuario puede activar y desactivar la firma S/MIME	Esta configuración especifica si un usuario tiene permiso para activar o desactivar la firma S/MIME. Esta configuración es válida únicamente si se ha seleccionado la opción "Activar S/MIME".
El usuario puede cambiar las credenciales de firma	Esta configuración especifica si un usuario puede anular las credenciales de firma. Esta configuración es válida únicamente si se ha seleccionado la opción "Activar S/MIME".
Activar cifrado de mensajes de S/MIME	En la configuración se especifica si desea que un dispositivo cifre los mensajes de correo de salida con el cifrado S/MIME. Esta configuración es válida únicamente si se ha seleccionado la opción "Activar S/MIME".
Credenciales de cifrado	Esta configuración especifica cómo los dispositivos encuentran los certificados necesarios para cifrar los mensajes. Valores posibles: • Certificado compartido • SCEP • Credencial de usuario Después de seleccionar el tipo de perfil, seleccione el certificado compartido, el SCEP o el perfil de credenciales de usuario que desea utilizar. Esta configuración es válida únicamente si se ha seleccionado la opción "Activar S/MIME".
Certificado compartido de cifrado	En la configuración se especifica el perfil de certificado compartido para un certificado de cliente que un dispositivo puede utilizar para cifrar mensajes de correo. Los dispositivos eligen el certificado adecuado para el destinatario para cifrar mensajes mediante S/MIME. Esta configuración es válida únicamente si se ha seleccionado la opción "Activar S/MIME".

iOS: configuración del perfil de correo	Descripción
SCEP de cifrado	Esta configuración especifica el perfil SCEP que los dispositivos pueden utilizar para recuperar los certificados necesarios para cifrar mensajes de correo mediante S/MIME. Esta configuración es válida únicamente si se ha seleccionado la opción "Activar S/MIME".
Credenciales de usuario de cifrado	Esta configuración especifica el perfil de credenciales de usuario que los dispositivos pueden utilizar para recuperar los certificados de clientes necesarios para cifrar mensajes de correo mediante S/MIME. Esta configuración es válida únicamente si se ha seleccionado la opción "Activar S/MIME".
El usuario puede anular el cifrado S/MIME	Esta configuración especifica si un usuario puede activar o desactivar la configuración de cifrado. Esta configuración es válida únicamente si se ha seleccionado la opción "Activar S/MIME".
El usuario puede anular las credenciales de cifrado S/MIME	Esta configuración especifica si un usuario puede anular las credenciales de cifrado S/MIME. Esta configuración es válida únicamente si se ha seleccionado la opción "Activar S/MIME".
Cifrar mensajes	Esta configuración especifica si se deben cifrar todos los mensajes de correo cuando el usuario los envía (Obligatorio) o si el usuario puede elegir qué mensajes cifrar a la hora de enviarlos (Permitir). Este ajuste se aplica únicamente si se ha seleccionado el ajuste "Activar S/MIME". Valores posibles: • Obligatorio • Permitir El valor predeterminado es "Obligatorio". Esta configuración es válida únicamente si se ha seleccionado la opción "Activar S/MIME".

iOS: configuración del perfil de correo	Descripción
Días para sincronizar	En la configuración se especifica el número de días transcurridos para sincronizar los mensajes de correo y los datos del organizador en un dispositivo. Valores posibles: • 1 día • 3 días • 7 días • 14 días • 1 mes • Indefinidamente El valor predeterminado es "7 días". **Nota:** La configuración se aplica únicamente al correo predeterminado y las aplicaciones del organizador en los dispositivos con el tipo de activación Controles de MDM.
VPN por cuenta	Esta configuración especifica el perfil de VPN que se utiliza para la comunicación de red de esta cuenta. Esta configuración se aplica únicamente a dispositivos con iOS 14 o versiones posteriores y a dispositivos iPadOS 14 y versiones posteriores.
Autenticación	
Activar BlackBerry Secure Gateway	Esta configuración especifica si los dispositivos con el tipo de activación Controles de MDM utilizan BlackBerry Secure Gateway para conectarse al servidor de correo. El BlackBerry Secure Gateway proporciona una conexión segura al servidor de correo de su empresa a través del BlackBerry Infrastructure y BlackBerry UEM. Si ha configurado grupos de servidores para dirigir el tráfico de BlackBerry Secure Gateway a una conexión regional determinada de BlackBerry Infrastructure, debe asociar el perfil de correo electrónico con el grupo de servidores correspondiente.
Tipo de autenticación	En la configuración se especifica el tipo de autenticación que un dispositivo utiliza para conectarse al servidor de correo. Esta configuración es válida únicamente si no se ha seleccionado la opción "Activar BlackBerry Secure Gateway". Valores posibles: • Ninguno • Certificado compartido • SCEP • Credencial de usuario El valor predeterminado es "Ninguno".

iOS: configuración del perfil de correo	Descripción
Perfil de certificado compartido	En la configuración se especifica el perfil de certificado compartido para un certificado de cliente que un dispositivo utiliza para conectar con el servidor de correo. Esta configuración es válida únicamente si no se ha seleccionado la opción "Activar BlackBerry Secure Gateway" y la opción "Tipo de autenticación" se establece en "Certificado compartido".
Perfil SCEP asociado	En esta configuración se especifica el perfil SCEP asociado que utiliza un dispositivo para inscribir un certificado de cliente con el objetivo de autenticarlo con el servidor de correo. Esta configuración es válida únicamente si no se ha seleccionado la opción "Activar BlackBerry Secure Gateway" y la opción "Tipo de autenticación" se establece en "SCEP".
Perfil de credenciales de usuario asociado	En la configuración se especifica el perfil de credenciales de usuario asociado que un dispositivo debe utilizar para inscribir un certificado de cliente con el objetivo de autenticarlo con el servidor de correo. Esta configuración es válida únicamente si la opción "Tipo de autenticación" se establece en "Credenciales del usuario".
Utilizar credenciales y certificado	Esta configuración especifica si un dispositivo utiliza las credenciales y un certificado de cliente obtenido mediante el perfil SCEP asociado para autenticar con el servidor de correo. Esta configuración es válida únicamente si no se ha seleccionado la opción "Activar BlackBerry Secure Gateway" y la opción "Tipo de autenticación" se establece en "SCEP".
Utilizar OAuth para la autenticación	En esa configuración se especifica si la conexión debe utilizar OAuth para la autenticación.
URL de inicio de sesión OAuth	Esta configuración especifica la URL que esta cuenta debe utilizar para iniciar sesión en OAuth. Cuando se especifica esta URL, se debe especificar un host porque no se utiliza la detección automática. Esta configuración es válida únicamente si no se ha seleccionado la opción "Activar BlackBerry Secure Gateway".
URL de solicitud de token OAuth	Esta configuración especifica la URL que esta cuenta debe utilizar para las solicitudes de token mediante OAuth Esta configuración es válida únicamente si no se ha seleccionado la opción "Activar BlackBerry Secure Gateway".
Utilizar SSL	Esta configuración especifica si un dispositivo debe utilizar SSL para conectarse al servidor de correo.

iOS: configuración del perfil de correo	Descripción
Aceptar todos los certificados SSL	Esta configuración especifica si se aceptan todos los certificados SSL. Esta configuración es válida únicamente si se ha seleccionado la opción "Utilizar SSL".
Dominios de correo electrónico externos	
Lista de dominios de correo externos permitidos	Esta configuración especifica la lista de dominios a los que un usuario puede enviar el correo de trabajo o las entradas de calendario. Por ejemplo, cuando un usuario agrega un destinatario que tiene una dirección de correo en el dominio permitido a un mensaje de correo o a una entrada de calendario, no se muestra ningún mensaje de advertencia. La configuración se aplica solo al espacio de trabajo. Si incluye varios nombres de dominio, sepárelos con una coma (,), un punto y coma (;) o un espacio.
Lista de dominios de correo externos restringidos	Esta configuración especifica la lista de dominios a los que los usuarios no pueden enviar el correo de trabajo o las entradas de calendario. Por ejemplo, si un usuario intenta agregar un destinatario con una dirección de correo del dominio restringido a un mensaje de correo o a una invitación de calendario, la aplicación Work Connect impide que el usuario complete la tarea. La configuración se aplica solo al espacio de trabajo. Si incluye varios nombres de dominio, sepárelos con una coma (,), un punto y coma (;) o un espacio.
Servicios activados	
Correo	Esta configuración especifica si los usuarios pueden acceder a sus correos electrónicos del trabajo desde sus dispositivos.
Contactos	Esta configuración especifica si los usuarios pueden acceder a sus contactos del trabajo desde sus dispositivos.
Calendarios	Esta configuración especifica si los usuarios pueden acceder a sus calendarios del trabajo desde sus dispositivos.
Recordatorios	Esta configuración especifica si los usuarios pueden acceder a sus recordatorios del trabajo desde sus dispositivos.
Notas	Esta configuración especifica si los usuarios pueden acceder a sus notas del trabajo desde sus dispositivos.
Modificación de cuenta	
Correo	Esta configuración especifica si los usuarios pueden activar o desactivar el acceso al correo electrónico del trabajo desde el dispositivo.
Contactos	Esta configuración especifica si los usuarios pueden activar o desactivar el acceso a los contactos del trabajo desde el dispositivo.

iOS: configuración del perfil de correo	Descripción
Calendarios	Esta configuración especifica si los usuarios pueden activar o desactivar el acceso al calendario del trabajo desde el dispositivo.
Recordatorios	Esta configuración especifica si los usuarios pueden activar o desactivar el acceso a los recordatorios del trabajo desde el dispositivo.
Notas	Esta configuración especifica si los usuarios pueden activar o desactivar el acceso a las notas del trabajo desde el dispositivo.

macOS: configuración del perfil de correo

macOS aplica perfiles a las cuentas de usuario o los dispositivos. Los perfiles de correo se aplican a cuentas de usuario.

macOS: configuración del perfil de correo	Descripción
Ruta	En la configuración se especifica la ruta de red del servidor de correo.
Puerto	En la configuración se especifica el puerto que se utiliza para conectarse al servidor de correo.
Utilizar SSL	En la configuración se especifica si un dispositivo debe utilizar SSL para conectarse al servidor de correo.
Nombre de host externo o dirección IP	En la configuración se especifica el nombre de host externo o la dirección IP del servidor de correo.
Utilizar SSL externo	En la configuración se especifica si un dispositivo debe utilizar SSL para conectarse al servidor de correo externo.
Ruta externa	En la configuración se especifica la ruta de red del servidor de correo externo.
Puerto del servidor externo	En la configuración se especifica el puerto que se utiliza para conectarse al servidor de correo externo.

Android: Configuración del perfil de correo electrónico

Android: Configuración del perfil de correo electrónico	Descripción
Configuración de entrega	

Android: Configuración del perfil de correo electrónico	Descripción
Tipo de perfil	Esta configuración especifica si desea que este perfil sea compatible con Exchange ActiveSync o IBM Notes Traveler. Valores posibles: • Exchange ActiveSync • IBM Notes Traveler El valor predeterminado es "Exchange ActiveSync".
Días para sincronizar	Esta configuración especifica el número de días transcurridos para sincronizar los mensajes de correo electrónico y los datos del organizador en un dispositivo Android con el tipo de activación Controles de MDM. Valores posibles: • Ilimitado • 1 día • 3 días • 7 días • 14 días • 1 mes El valor predeterminado es "1 mes". Para los dispositivos Android que utilizan Samsung Knox MDM, si establece el valor en Ilimitado, solo se sincroniza un mes. **Nota:** La configuración se aplica únicamente al correo predeterminado y las aplicaciones del organizador en los dispositivos Android con el tipo de activación Controles de MDM.
Tipo de autenticación	Esta configuración especifica el tipo de autenticación que un dispositivo Android utiliza para conectarse al servidor de correo. Valores posibles: • Ninguno • Certificado compartido • SCEP • Credencial de usuario El valor predeterminado es "Ninguno".
Perfil SCEP asociado	Esta configuración especifica el perfil SCEP asociado que un dispositivo Android debe utilizar para obtener un certificado de cliente con el objetivo de autenticarlo en el servidor de correo. Esta configuración es válida únicamente si la opción "Tipo de autenticación" se establece en "SCEP".

Android: Configuración del perfil de correo electrónico	Descripción
Utilizar credenciales y certificado	Esta configuración especifica si un dispositivo utiliza las credenciales y un certificado de cliente obtenido mediante el perfil SCEP asociado para autenticar con el servidor de correo. Esta configuración es válida únicamente si la opción "Tipo de autenticación" se establece en "SCEP".
Perfil de certificado compartido	Esta configuración especifica el perfil de certificado compartido para un certificado de cliente que el dispositivo Android utiliza para conectar con el servidor de correo. Esta configuración es válida únicamente si la opción "Tipo de autenticación" se establece en "Certificado compartido".
Perfil de credenciales de usuario asociado	Esta configuración especifica el perfil de credenciales de usuario para un certificado de cliente que el dispositivo Android utiliza para conectar con el servidor de correo. Esta configuración es válida únicamente si la opción "Tipo de autenticación" se establece en "Credenciales del usuario".
Utilizar SSL	Esta configuración especifica si un dispositivo debe utilizar SSL para conectarse al servidor de correo.
Aceptar todos los certificados SSL	Esta opción especifica si un dispositivo debe aceptar automáticamente certificados SSL que no sean de confianza procedentes del servidor de correo. Cuando esta opción no está seleccionada, los dispositivos solo se pueden conectar a los servidores de correo que utilizan un certificado SSL de confianza.
Tamaño máximo de archivo adjunto de correo	Esta configuración especifica el tamaño máximo permitido para los archivos adjuntos de correo (en MB). Los valores posibles son de 1 a 365. La configuración predeterminada es 25. La configuración se aplica únicamente a dispositivos Android Enterprise.
Firma de correo predeterminada para los nuevos mensajes	Esta configuración especifica una firma de correo que se agrega automáticamente a los mensajes de correo nuevos. La configuración se aplica únicamente a dispositivos Android Enterprise.
Activar S/MIME	Esta configuración especifica si los dispositivos pueden enviar mensajes de correo protegidos con S/MIME. Para los dispositivos que utilizan BlackBerry Productivity Suite, debe establecer un valor para la configuración "Compatibilidad de S/MIME" en su lugar.

Android: Configuración del perfil de correo electrónico	Descripción
Firmar mensajes	Esta configuración especifica si desea que los dispositivos envíen todos los mensajes de correo de salida con una firma digital. Esta configuración es válida únicamente si se ha seleccionado la opción "Activar S/MIME". Para los dispositivos Android Enterprise, esta configuración solo se aplica a los dispositivos que utilizan Dividir productividad. Para los dispositivos que utilizan BlackBerry Productivity Suite, debe establecer un valor para la configuración "Mensajes de S/MIME con firma digital" en su lugar.
Credenciales de firma	Esta configuración especifica las credenciales que un dispositivo utiliza para firmar los mensajes de correo. Esta configuración es válida únicamente si se ha seleccionado la opción "Firmar mensajes". Valores posibles: • Certificado compartido • SCEP • Credencial de usuario La configuración predeterminada es "Certificado compartido".
Certificado compartido de firma	Esta configuración especifica el perfil de certificado compartido para un certificado de cliente que un dispositivo utiliza para firmar mensajes de correo. Esta configuración es válida únicamente si la opción "Credenciales de firma" se establece en "Certificado compartido".
SCEP de firma	Esta configuración especifica el perfil SCEP para un certificado de cliente que un dispositivo utiliza para firmar mensajes de correo. Esta configuración es válida únicamente si la opción "Credenciales de firma" se establece en "SCEP".
Credenciales de usuario de firma	Esta configuración especifica el perfil de credenciales de usuario para un certificado de cliente que un dispositivo utiliza para firmar mensajes de correo. Esta configuración es válida únicamente si la opción "Credenciales de firma" se establece en "Credenciales del usuario".
Cifrar mensajes	Esta configuración especifica si desea que los dispositivos cifren los mensajes de correo de salida con el cifrado S/MIME. Esta configuración es válida únicamente si se ha seleccionado la opción "Activar S/MIME". Para los dispositivos Android Enterprise, esta configuración solo se aplica a los dispositivos que utilizan Dividir productividad. Para los dispositivos que utilizan BlackBerry Productivity Suite, debe establecer un valor para la configuración "Mensajes de S/MIME con firma digital" en su lugar.

Android: Configuración del perfil de correo electrónico	Descripción
Credenciales de cifrado	Esta configuración especifica las credenciales que un dispositivo utiliza para cifrar los mensajes de correo. Esta configuración es válida únicamente si se ha seleccionado la opción "Cifrar mensajes". Valores posibles: • Certificado compartido • SCEP • Credencial de usuario La configuración predeterminada es "Certificado compartido".
Certificado compartido de cifrado	Esta configuración especifica el perfil de certificado compartido para un certificado de cliente que un dispositivo utiliza para cifrar mensajes de correo. Esta configuración es válida únicamente si la opción "Credenciales de cifrado" se establece en "Certificado compartido".
SCEP de cifrado	Esta configuración especifica el perfil SCEP para un certificado de cliente que un dispositivo utiliza para cifrar mensajes de correo. Esta configuración es válida únicamente si la opción "Credenciales de firma" se establece en "SCEP".
Credenciales de usuario de cifrado	Esta configuración especifica el perfil de credenciales de usuario para un certificado de cliente que un dispositivo utiliza para cifrar mensajes de correo. Esta configuración es válida únicamente si la opción "Credenciales de firma" se establece en "Credenciales del usuario".
Requerir autenticación de la tarjeta inteligente para el correo	Esta configuración especifica si se necesita una tarjeta inteligente para los dispositivos Samsung Knox para autenticar con el servidor de correo.
Permitir al usuario editar la configuración	Especifique si el usuario puede editar la configuración de entrega. La configuración se aplica únicamente a dispositivos Samsung Knox.
Dominios de correo electrónico externos	
Lista de dominios de correo externos permitidos	Esta configuración especifica la lista de dominios a los que un usuario puede enviar el correo de trabajo o las entradas de calendario. Por ejemplo, cuando un usuario agrega un destinatario que tiene una dirección de correo en el dominio permitido a un mensaje de correo o a una entrada de calendario, no se muestra ningún mensaje de advertencia. La configuración se aplica solo al espacio de trabajo. Si incluye varios nombres de dominio, sepárelos con una coma (,), un punto y coma (;) o un espacio.

Android: Configuración del perfil de correo electrónico	Descripción
Lista de dominios de correo externos restringidos	Esta configuración especifica la lista de dominios a los que los usuarios no pueden enviar el correo de trabajo o las entradas de calendario. Por ejemplo, si un usuario intenta agregar un destinatario con una dirección de correo del dominio restringido a un mensaje de correo o a una invitación de calendario, la aplicación Correo o la aplicación Calendario impide que el usuario complete la tarea. La configuración se aplica solo al espacio de trabajo. Si incluye varios nombres de dominio, sepárelos con una coma (,), un punto y coma (;) o un espacio.

Windows: configuración del perfil de correo

Windows: configuración del perfil de correo	Descripción
Configuración de entrega	
Tipo de perfil	En la configuración se especifica si desea que este perfil sea compatible con Exchange ActiveSync o IBM Notes Traveler. Valores posibles: • Exchange ActiveSync • IBM Notes Traveler El valor predeterminado es "Exchange ActiveSync".
Nombre de cuenta	En la configuración se especifica el nombre de la cuenta de correo de trabajo que aparece en el dispositivo Windows. Puede utilizar una variable como, por ejemplo, %UserEmailAddress%.
Intervalo de sincronización	En la configuración se especifica la frecuencia con que un dispositivo Windows descarga mensajes de correo del servidor de correo. Valores posibles: • A medida que se reciben los elementos • Manual • 15 minutos • 30 minutos • 60 minutos El valor predeterminado es "A medida que se reciben los elementos".

Windows: configuración del perfil de correo	Descripción
Días para sincronizar	En la configuración se especifica el número de días transcurridos para sincronizar los mensajes de correo y los datos del organizador en un dispositivo Windows. Valores posibles: • Indefinidamente • 3 días • 7 días • 14 días • 1 mes El valor predeterminado es "7 días".
Utilizar SSL	En la configuración se especifica si un dispositivo Windows debe utilizar SSL para conectarse al servidor de correo.
Contenido para sincronizar	
Correo	En la configuración se especifica si desea que un dispositivo Windows sincronice los mensajes de correo con el servidor de correo.
Contactos	En la configuración se especifica si desea que un dispositivo Windows sincronice los contactos con el servidor de correo.
Calendario de	En la configuración se especifica si desea que un dispositivo Windows sincronice las entradas de calendario con el servidor de correo.
Tarea	En la configuración se especifica si desea que un dispositivo Windows sincronice los datos de tareas con el servidor de correo. Esta configuración es válida únicamente si la opción "Tipo de perfil" se establece en "Exchange ActiveSync".

Protección de los datos de correo electrónico enviados a dispositivos con iOS mediante BlackBerry Secure Gateway

BlackBerry Secure Gateway proporciona una conexión segura a través de BlackBerry Infrastructure y BlackBerry UEM al servidor de correo electrónico de su empresa para dispositivos con iOS y iPadOS que están activados con Controles de MDM.

Si tiene previsto usar BlackBerry Secure Gateway, debe comprobar que su empresa cuente con las licencias de correspondientes. Para obtener más información, consulte el contenido sobre licencias.

La activación de BlackBerry Secure Gateway permite a los dispositivos enviar y recibir correo electrónico de trabajo sin tener que exponer su servidor de correo fuera del firewall o ubicar el servidor de correo en una DMZ. Para activar BlackBerry Secure Gateway, seleccione la configuración "Activar BlackBerry Secure Gateway" en el perfil de correo electrónico.

Si su entorno incluye dispositivos con iOS o iPadOS 13.0 o posteriores y el servidor de correo electrónico de su empresa está configurado para utilizar la autenticación moderna de Microsoft, debe seleccionar la configuración "Usar OAuth para la autenticación" en el perfil de correo electrónico y configurar BlackBerry Secure Gateway para usar OAuth para la autenticación con el servidor de correo.

Si ha configurado grupos de servidores para admitir conexiones regionales con BlackBerry Infrastructure, puede dirigir el tráfico de BlackBerry Secure Gateway a una conexión regional específica mediante la asociación del perfil de correo electrónico con el grupo de servidores apropiado.

Configuración de las conexiones seguras para su servidor de correo electrónico cuando se activa BlackBerry Secure Gateway

Si activa BlackBerry Secure Gateway para proporcionar una conexión segura a través de BlackBerry UEM entre el servidor de correo de su empresa y los dispositivos con iOS y iPadOS con el tipo de activación Controles de MDM, es posible que deba configurar BlackBerry UEM para establecer conexiones TLS/SSL con Exchange ActiveSync o con el proveedor de identidad Active Directory.

Si su entorno incluye dispositivos con iOS y iPadOS 13.0 o posterior y que utilizan un sistema de autenticación moderno para conectarse a Microsoft Exchange Online, debe agregar el certificado (o el certificado raíz) del proveedor de identidad a BlackBerry UEM. BlackBerry Secure Gateway requiere que el certificado confíe en el proveedor de identidad cuando establece la conexión. También deberá especificar el extremo de detección y el recurso del servidor de correo para la autenticación moderna

Si el servidor de Exchange ActiveSync está configurado para exigir una conexión TLS, debe agregar el certificado de servidor (o su certificado raíz) de Exchange ActiveSync a BlackBerry UEM. BlackBerry Secure Gateway requiere que el certificado confíe en el servidor de Exchange ActiveSync cuando establece la conexión TLS/SSL. En función de los requisitos de seguridad del servidor de Exchange ActiveSync, es posible que también deba actualizar la lista de versiones y cifrados TLS que BlackBerry Secure Gateway puede utilizar para la autenticación con Exchange ActiveSync.

Configuración de BlackBerry UEM para que confíe en el certificado del servidor Exchange ActiveSync y en el proveedor de identidad

Antes de empezar:

Exporte el certificado en formato X.509 (*.cer y *.der) desde los siguientes servidores y guárdelo en una ubicación de red a la que pueda acceder desde la consola de administración:

- Servidor de Exchange ActiveSync
- proveedor de identidad de Active Directory, si su entorno incluye iOS o iPadOS 13.0 y admite la autenticación moderna.

1. En la barra de menús, haga clic en **Configuración > Integración externa > Certificados de confianza**.
2. Haga clic + junto a **Elementos de confianza del servidor Exchange ActiveSync**.
3. Haga clic en **Examinar**.
4. Seleccione el archivo de certificado que desea utilizar.
5. Haga clic en **Abrir**.
6. Escriba una descripción para el certificado.
7. Haga clic en **Agregar**.

Configuración de BlackBerry Secure Gateway para usar las versiones y los cifrados de TLS que admite u OAuth

Puede activar BlackBerry Secure Gateway para utilizar OAuth para la autenticación moderna. Para utilizar OAuth, necesita el extremo del documento de detección del proveedor de identidad y la URL del servidor de correo. Para obtener más información sobre el documento de detección, consulte la documentación de Microsoft.

También puede especificar la versión de TLS y Microsoft Exchange los cifrados SSL que BlackBerry Secure Gateway utiliza para las conexiones a Exchange ActiveSync.

1. En la barra de menús, haga clic en **Configuración > Integración externa > BlackBerry Secure Gateway**.
2. Para agregar o eliminar una versión TLS o un cifrado SSL, haga clic + en la tabla correspondiente.
3. Haga clic en la versión o el cifrado de TLS que desee agregar o eliminar de la lista **Seleccionado**.
4. Haga clic en la flechas para mover el elemento a la lista que desee.
5. Haga clic en **Asignar**.
6. Para utilizar la autenticación moderna, seleccione **Activar OAuth para la autenticación del servidor de correo**.
7. En el campo **Extremo de detección**, introduzca la URL que BlackBerry Secure Gateway utiliza para recuperar y almacenar en caché el documento de detección del proveedor de identidad.

   La URL debe tener el formato https://<*proveedor de identidad*>/.well-known/openid-configuration (por ejemplo, `https://login.microsoftonline.com/common/.well-known/openid-configuration`). BlackBerry Secure Gateway recupera tanto los documentos de detección no versionados como v2.0 y actualiza periódicamente los documentos almacenados en caché.
8. En el campo **Recurso del servidor de correo**, introduzca la URL del servidor de correo especificado en el perfil de correo electrónico, comenzando con "https://" (por ejemplo, `https://outlook.office365.com`).
9. Haga clic en **Guardar**.

Activación de BlackBerry Hub unificado en dispositivos Android Enterprise

BlackBerry Hub es una aplicación Android que permite a los usuarios ver los mensajes, las notificaciones y los eventos en un solo lugar.

Para permitir que los usuarios con dispositivos Android Enterprise puedan ver tanto los mensajes personales como los de trabajo en BlackBerry Hub, es necesario verificar algunos ajustes en BlackBerry UEM.

1. Para la política de TI asignada a los usuarios, en la sección BlackBerry Productivity Suite, verifique que la regla de política de TI "Permitir vista de cuentas unificada en BlackBerry Hub" está seleccionada.
2. En la configuración de la aplicación para BlackBerry Hub, compruebe que se han seleccionado los siguientes elementos:
   - IPC entre perfiles
   - Acceder al contenido de trabajo

Después de terminar:

Para obtener información acerca del uso de BlackBerry Hub en dispositivos, como agregar una cuenta de correo electrónico o personalizar la configuración de BlackBerry Hub, consulte el contenido de BlackBerry Hub.

Para obtener información sobre la resolución de problemas, visite http://support.blackberry.com/community y lea el artículo 37721.

Ampliación de la seguridad del correo mediante S/MIME

Puede ampliar la seguridad del correo para los usuarios de dispositivos con iOS y Android al activar S/MIME. S/MIME proporciona un método estándar para cifrar y firmar mensajes de correo. Los usuarios pueden cifrar, firmar o cifrar y firmar mensajes de correo utilizando la protección S/MIME cuando utilizan una cuenta de correo de trabajo que admita mensajes protegidos con S/MIME en los dispositivos. S/MIME no se puede activar para las direcciones de correo personales.

Los usuarios pueden guardar los certificados S/MIME del destinatario en sus dispositivos. Los usuarios pueden almacenar sus claves privadas en sus dispositivos o en una tarjeta inteligente.

Active S/MIME para los usuarios en un perfil de correo. No puede forzar a los usuarios de dispositivos con iOS ni Android a utilizar S/MIME. Cuando el uso de S/MIME es opcional, un usuario puede activar S/MIME en el dispositivo y especificar si desea cifrar, firmar o cifrar y firmar mensajes de correo.

La configuración S/MIME tiene prioridad sobre la configuración de PGP. Cuando la compatibilidad de S/MIME se establece en "Obligatorio", los ajustes de PGP se ignoran.

Recuperación de certificados S/MIME

Puede utilizar perfiles de recuperación de certificados que permitan a los dispositivos Android y iOS buscar y recuperar los certificados S/MIME de los destinatarios desde los servidores de certificados LDAP. Si el certificado S/MIME todavía no está en el almacén de certificados del dispositivo, el dispositivo lo recupera y lo importa automáticamente al almacén de certificados.

Los dispositivos Android y iOS buscan cada servidor de certificados LDAP que se especifique en el perfil y recuperan el certificado S/MIME. Si hay más de un certificado S/MIME y un dispositivo no puede determinar el preferido, el dispositivo muestra todos los certificados S/MIME para que el usuario pueda seleccionar el que desea utilizar.

Puede solicitar que los dispositivos utilicen tanto la autenticación simple como la autenticación Kerberos con los servidores de certificados LDAP. Si solicita que los dispositivos utilicen la autenticación simple, puede incluir las credenciales de autenticación necesarias en los perfiles de recuperación de certificado de modo que los dispositivos puedan autenticarse automáticamente con los servidores de certificados LDAP. Si solicita que los dispositivos utilicen la autenticación Kerberos, puede incluir las credenciales de autenticación necesarias en los perfiles de recuperación de certificado de modo que los dispositivos Android y iOS puedan autenticarse automáticamente con los servidores de certificados LDAP. De lo contrario, el dispositivo solicitará al usuario las credenciales de autenticación necesarias la primera vez que el dispositivo intente autenticarse en un servidor de certificados LDAP.

Si implementa la autenticación Kerberos para la recuperación de certificados S/MIME, debe asignar un perfil de inicio de sesión único aplicable a los usuarios o grupos de usuarios aplicables. Para obtener más información sobre cómo crear y asignar un perfil de registro único, consulte Configuración de la autenticación de registro único de los dispositivos.

Si no crea un perfil de recuperación de certificados y lo asigna a cuentas de usuario, a grupos de usuarios o a grupos de dispositivos, los usuarios deberán importar manualmente los certificados S/MIME desde un archivo adjunto al correo de trabajo o desde un equipo.

Creación de un perfil de recuperación de certificados

Antes de empezar:

- Para permitir que los dispositivos puedan confiar en los servidores de certificados LDAP cuando hacen conexiones seguras, puede que necesite distribuir certificados de CA en los dispositivos. Si es necesario, cree

los perfiles de certificado de CA y asígnelos a las cuentas de usuarios, a los grupos de usuarios o a los grupos de dispositivos. Para obtener más información sobre los certificados de CA, consulte Envío de certificados de CA a dispositivos y aplicaciones.

- Si implementa la autenticación Kerberos para la recuperación de certificados S/MIME, debe asignar un perfil de inicio de sesión único aplicable a los usuarios o grupos de usuarios aplicables. Para obtener más información sobre los perfiles de registro único, consulte Configuración de la autenticación de registro único de los dispositivos.

1. En la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Certificados > Recuperación de certificado**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil de recuperación de certificados.
5. En la tabla, haga clic en +.
6. En el campo **URL de servicio**, escriba el servidor de certificados FQDN o LDAP con el formato ldap://<*fqdn*>:<*puerto*>. (Por ejemplo, ldap://server01.example.com:389).
7. En el campo **Base de búsqueda**, escriba el DN de base que sea el punto de partida para las búsquedas del servidor de certificados LDAP.
8. En la lista desplegable **Ámbito de búsqueda**, lleve a cabo una de las siguientes acciones:
   - Para buscar solo el objeto base (DN de base), haga clic en **Base**. Esta opción es el valor predeterminado.
   - Para buscar en un nivel por debajo del objeto base, pero no el objeto base, haga clic en **Un nivel**.
   - Para buscar el objeto base y todos los niveles por debajo, haga clic en **Subárbol**.
   - Para buscar en todos los niveles por debajo del objeto base, pero no el objeto base, haga clic en **Secundario**.
9. Si se necesita autenticación, realice las acciones siguientes:
   a) En la lista desplegable **Tipo de autenticación**, haga clic en **Simple** o en **Kerberos**.
   b) En el campo **ID de usuario de LDAP**, escriba el DN de una cuenta que disponga de permisos de búsqueda en el servidor de certificados LDAP (por ejemplo, cn=admin,dc=ejemplo,dc=com).
   c) En el campo **Contraseña de LDAP**, escriba la contraseña de la cuenta que tenga permisos de búsqueda en el servidor de certificados LDAP.
10. Si fuera necesario, seleccione la casilla de verificación **Usar conexión segura**.
11. En el campo **Tiempo de espera de conexión**, escriba la cantidad de tiempo, en segundos, que el dispositivo espera la respuesta del servidor de certificados LDAP.
12. Haga clic en **Agregar**.
13. Repita los pasos del 5 al 11 para cada servidor de certificados LDAP.
14. Haga clic en **Agregar**.

Después de terminar:

- Si fuera necesario, clasifique los perfiles.

Determinación del estado de los certificados S/MIME en dispositivos

Puede utilizar perfiles CRL y OCSP para permitir que los dispositivos con iOS y Android comprueben el estado de los certificados S/MIME. Se puede asignar un perfil OCSP y uno CRL a cuentas de usuarios, a grupos de usuarios y a grupos de dispositivos.

Los dispositivos con iOS y Android buscan cada respondedor OCSP que especifica en un perfil OCSP y recuperan el estado del certificado S/MIME. Los dispositivos con que iOS y Android pueden enviar solicitudes de estado de

certificado a BlackBerry UEM, y puede utilizar perfiles CRL para configurar BlackBerry UEM para buscar el estado de los certificados S/MIME mediante HTTP, HTTPS o LDAP.

Si se utiliza Exchange ActiveSync para la recuperación del certificado, los dispositivos iOS y Android utilizarán Exchange ActiveSync para verificar el estado de los certificados S/MIME. Si se utiliza LDAP para la recuperación del certificado, los dispositivos iOS y Android utilizarán OCSP para verificar el estado de los certificados. Los dispositivos iOS y Android no utilizan perfiles OCSP. Los dispositivos verifican el respondedor OCSP con el certificado.

Para obtener más información sobre los indicadores de estado del certificado, consulte la guía de usuario del dispositivo para conocer los detalles acerca de los iconos de correo electrónico seguros.

Creación de un perfil OCSP

Los perfiles OCSP son compatibles con los dispositivos con iOS y Android.

1. En la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Certificados > OCSP**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil OCSP.
5. Realice las acciones siguientes:
   a) En la tabla, haga clic en +.
   b) En el campo **URL de servicio**, escriba la dirección web de un respondedor OCSP.
   c) En el campo **Tiempo de espera de conexión**, escriba la cantidad de tiempo, en segundos, que el dispositivo espera la respuesta de OCSP.
   d) Haga clic en **Agregar**.
6. Repita el paso 4 para cada respondedor OCSP.
7. Haga clic en **Agregar**.

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

Creación de un perfil CRL

Los perfiles CRL son compatibles con los dispositivos con iOS y Android.

1. En la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Certificados > CRL**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil CRL.
5. Para permitir que los dispositivos puedan utilizar las URL de respondedor definidas en el certificado, seleccione la casilla de verificación **Usar respondedores de extensión de certificado**.
6. Lleve a cabo cualquiera de las tareas siguientes:

Tarea	Pasos
Especificación de la configuración CRL de HTTP	**a.** En la sección **HTTP para CRL**, haga clic en +. **b.** Escriba un nombre y una descripción para la configuración CRL de HTTP. **c.** En el campo **URL de servicio**, escriba la dirección web de un servidor HTTP o HTTPS. **d.** Haga clic en **Agregar**. **e.** Repita los pasos del 1 al 4 para cada servidor HTTP o HTTPS.
Especificación de la configuración CRL de LDAP	**a.** En la sección **LDAP para CRL**, haga clic en +. **b.** Escriba un nombre y una descripción para la configuración CRL de LDAP. **c.** En el campo **URL de servicio**, escriba el servidor FQDN o LDAP con el formato ldap://<*fqdn*>:<*puerto*> (por ejemplo, ldap://server01.example.com:389). Para conexiones seguras, utilice el formato ldaps://<*fqdn*>:<*puerto*>. **d.** En el campo **Base de búsqueda**, escriba el DN de base que sea el punto de partida para las búsquedas del servidor LDAP. **e.** Si fuera necesario, seleccione la casilla de verificación **Usar conexión segura**. **f.** En el campo **ID de usuario de LDAP**, escriba el DN de una cuenta que disponga de permisos de búsqueda en el servidor LDAP (por ejemplo, cn=admin,dc=ejemplo,dc=com). **g.** En el campo **Contraseña de LDAP**, escriba la contraseña de la cuenta que tenga permisos de búsqueda en el servidor LDAP. **h.** Haga clic en **Agregar**. **i.** Repita los pasos del 1 al 8 para cada servidor LDAP.

7. Haga clic en **Agregar**.

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

Ampliación de la seguridad del correo mediante PGP

Puede ampliar la seguridad del correo para los usuarios de dispositivos con iOS y Android activando PGP. PGP protege los mensajes de correo en dispositivos mediante el formato OpenPGP. Los usuarios pueden firmar, cifrar o firmar y cifrar mensajes de correo con la protección PGP al utilizar una dirección de correo de trabajo. PGP no se puede activar para las direcciones de correo personales.

Active PGP para los usuarios en un perfil de correo. Puede forzar a los usuarios del dispositivo con iOS y Android a utilizar PGP, no permitir el uso de PGP o hacerlo opcional. Cuando el uso de PGP es opcional (el valor predeterminado), un usuario puede activar PGP en el dispositivo y especificar si desea cifrar, firmar o cifrar y firmar mensajes de correo.

Para firmar y cifrar mensajes de correo, los usuarios deben guardar claves PGP para cada destinatario en sus dispositivos. Los usuarios pueden guardar claves PGP importando los archivos desde un mensaje de correo de trabajo.

Puede configurar PGP mediante las configuraciones del perfil de correo adecuadas.

Aplicación de un correo protegido mediante la clasificación de mensajes

La clasificación de mensajes permite a la empresa especificar e imponer políticas de correo electrónico seguras y agregar marcas visuales a los mensajes de correo electrónico en los dispositivos con iOS y Android. Puede utilizar BlackBerry UEM para proporcionar a los usuarios de dispositivos con iOS y Android opciones de clasificación de mensajes similares a las que están disponibles en las aplicaciones de correo electrónico de su ordenador. Puede definir las siguientes reglas a aplicar a los mensajes salientes, en función de las clasificaciones de los mensajes:

- Agregar una etiqueta para identificar la clasificación de mensajes (por ejemplo, Confidencial)
- Agregar un marcador visual al final de la línea del asunto (por ejemplo, [C])
- Agregar texto al principio o al final del cuerpo de un mensaje de correo electrónico (por ejemplo, "Este mensaje ha sido clasificado como confidencial")
- Configurar S/MIME o las opciones de PGP (por ejemplo, firmar y cifrar)
- Configurar una clasificación predeterminada

En dispositivos con iOS y Android, puede utilizar la clasificación de mensajes para solicitar a los usuarios que firmen, cifren o que firmen y cifren los mensajes de correo, así como para agregar marcas visuales a los mensajes de correo que envían desde sus dispositivos. Puede utilizar perfiles de correo para especificar la configuración de clasificación de mensajes (con extensiones de nombre de archivo .json) para enviar a los dispositivos de los usuarios. Cuando los usuarios responden a los mensajes de correo que tienen la clasificación de mensajes configurada o bien redacta los mensajes de correo protegido, la configuración de la clasificación de mensajes determina las reglas de clasificación que los dispositivos deben aplicar al mensaje saliente.

Las opciones de protección de mensajes en un dispositivo se limitan a los tipos de cifrado y firma digital que se permiten en el dispositivo. Cuando un usuario aplica una clasificación de mensajes a un mensaje de correo electrónico en el dispositivo, el usuario debe seleccionar uno de los tipos de protección de mensajes que permite dicha clasificación o aceptar el tipo de protección de mensajes predeterminado. Si un usuario selecciona una clasificación de mensajes que requiere la firma, el cifrado, o la firma y el cifrado del mensaje, y si el dispositivo no tiene configurado S/MIME o PGP, el usuario no puede enviar el mensaje de correo electrónico.

Los ajustes de S/MIME y de PGP tienen prioridad sobre los mensajes de clasificación. Los usuarios pueden aumentar, pero no reducir, los niveles de clasificación de los mensajes en sus dispositivos. Los niveles de clasificación de los mensajes están determinados por las reglas de correo electrónico seguro de cada clasificación.

Cuando la clasificación de mensajes está activada, los usuarios no pueden utilizar BlackBerry Assistant para enviar mensajes de correo desde los dispositivos.

Puede configurar la clasificación de mensajes mediante las adecuadas configuraciones del perfil de correo.

Para obtener más información acerca de cómo crear archivos de configuración de clasificación de mensajes, support.blackberry.com/community y lea el artículo 36736.

Creación de un perfil de correo IMAP/POP3

Los perfiles de correo IMAP/POP3 especifican cómo se conectan los dispositivos con iOS, macOS, Android y Windows a los servidores de correo IMAP o POP3 y sincronizan los mensajes de correo.

La configuración del perfil obligatorio varía para cada tipo de dispositivo y depende de los ajustes que seleccione.

Nota: BlackBerry UEM envía el perfil de correo a los dispositivos Android, pero el usuario debe configurar manualmente la conexión con el servidor de correo.

1. En la barra de menú, haga clic en **Políticas y perfiles**.
2. Haga clic en **Correo, Calendario y contactos > Correo IMAP/POP3**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil.
5. En el campo **Tipo de correo**, seleccione el tipo de protocolo de correo.
6. En el campo **Dirección de correo**, realice una de las siguientes acciones:
   - Si el perfil es para un usuario, escriba la dirección de correo del usuario.
   - Si el perfil es para varios usuarios, escriba `%UserEmailAddress%`.
7. En la sección **Configuración del correo electrónico entrante**, escriba el nombre de host o la dirección IP del servidor de correo para recibir el correo.
8. Si fuera necesario, escriba el puerto para recibir correo.
9. En el campo **Nombre de usuario**, realice una de las siguientes acciones:
   - Si el perfil es para un usuario, escriba el nombre de usuario.
   - Si el perfil es para varios usuarios, escriba `%UserName%`.
10. En la sección **Configuración del correo saliente**, escriba el nombre de host o la dirección IP del servidor de correo para enviar correo.
11. Si fuera necesario, escriba el puerto para enviar correo.
12. Si fuera necesario, seleccione **Autenticación requerida para el correo de salida** y especifique las credenciales utilizadas para enviar correo.
13. Haga clic en la pestaña de cada tipo de dispositivo de la empresa y configure los valores apropiados para cada configuración de perfil.
14. Haga clic en **Agregar**.

Configuración del perfil de correo IMAP/POP3

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. BlackBerry UEM admite variables predeterminadas que son variables predefinidas y personalizadas que se definen. Los perfiles de correo IMAP/POP3 son compatibles con los tipos de dispositivos siguientes:

- iOS
- macOS
- Android
- Windows

En algunos casos, la versión mínima del SO del dispositivo requerida para que sea compatible con una configuración es una versión no admitida por BlackBerry UEM. Para obtener más información acerca de las versiones compatibles, consulte la Matriz de compatibilidad.

iOS y macOS: Configuración del perfil de correo IMAP/POP3

Estos ajustes también se aplican a los dispositivos con iPadOS

macOS aplica perfiles a las cuentas de usuario o los dispositivos. Los perfiles IMAP/POP3 se aplican a las cuentas de usuario.

iOS: Configuración del perfil de correo IMAP/ POP3	Descripción
Prefijo de ruta IMAP	Si fuera necesario, esta configuración especifica el prefijo de la ruta de acceso de IMAP. Si fuera necesario, póngase en contacto con su ISP para obtener más información. Esta configuración solo es válida si el valor de la opción "Tipo de correo" se establece en "IMAP".
Permitir que los mensajes se muevan	Esta configuración especifica si desea que los usuarios puedan mover mensajes de correo desde esta cuenta a otra cuenta de correo en un dispositivo iOS.
Permitir la sincronización de direcciones recientes	Esta configuración especifica si un usuario de un dispositivo con iOS puede sincronizar direcciones de correo utilizadas recientemente en los dispositivos.
Utilizar solo con correo	Esta configuración especifica si desea que otras aplicaciones distintas de la aplicación de correo del dispositivo iOS puedan utilizar esta cuenta para enviar mensajes de correo.
Activar S/MIME	Esta configuración especifica si un usuario del dispositivo iOS puede enviar mensajes de correo protegidos con S/MIME. S/MIME solo es compatible con dispositivos que se activan con controles de MDM.
Credenciales de firma	Esta configuración especifica las credenciales que un dispositivo utiliza para firmar los mensajes de correo. Esta configuración es válida únicamente si se ha seleccionado la opción "Activar S/MIME". Valores posibles: • Certificado compartido • SCEP • Credencial de usuario La configuración predeterminada es "Certificado compartido".

iOS: Configuración del perfil de correo IMAP/ POP3	Descripción
Certificado compartido de firma	Esta configuración especifica el perfil de certificado compartido para un certificado de cliente que un dispositivo utiliza para firmar mensajes de correo. Esta configuración es válida únicamente si la opción "Credenciales de firma" se establece en "Certificado compartido".
SCEP de firma	Esta configuración especifica el perfil SCEP que los dispositivos pueden utilizar para recuperar los certificados necesarios para firmar mensajes de correo mediante S/MIME. Esta configuración es válida únicamente si la opción "Credenciales de firma" se establece en "SCEP".
Credenciales de usuario de firma	Esta configuración especifica el perfil de credenciales de usuario que los dispositivos pueden utilizar para obtener los certificados de clientes necesarios para firmar mensajes de correo mediante S/MIME. Esta configuración es válida únicamente si la opción "Credenciales de firma" se establece en "Credenciales del usuario".
Credenciales de cifrado	Esta configuración especifica cómo los dispositivos encuentran los certificados necesarios para cifrar los mensajes. Esta configuración es válida únicamente si se ha seleccionado la opción "Activar S/MIME". Valores posibles: • Certificado compartido • SCEP • Credencial de usuario Después de seleccionar el tipo de perfil, seleccione el certificado compartido, el SCEP o el perfil de credenciales de usuario que desea utilizar.
Certificado compartido de cifrado	Esta configuración especifica el perfil de certificado compartido para un certificado de cliente que un dispositivo utiliza para cifrar mensajes de correo. Los dispositivos eligen el certificado adecuado para el destinatario para cifrar mensajes mediante S/MIME. Esta configuración es válida únicamente si la opción "Credenciales de cifrado" se establece en "Certificado compartido".
SCEP de cifrado	Esta configuración especifica el perfil SCEP que los dispositivos pueden utilizar para recuperar los certificados necesarios para cifrar mensajes de correo mediante S/MIME. Esta configuración solo es válida si la opción "Credenciales de cifrado" se establece en "SCEP".

iOS: Configuración del perfil de correo IMAP/ POP3	Descripción
Credenciales de usuario de cifrado	Esta configuración especifica el perfil de credenciales de usuario que los dispositivos pueden utilizar para recuperar los certificados de clientes necesarios para cifrar mensajes de correo mediante S/MIME. Esta configuración solo es válida si la opción "Credenciales de cifrado" se establece en "Credenciales del usuario".
Cifrar mensajes	Esta configuración especifica si se deben cifrar todos los mensajes de correo cuando el usuario los envía (Obligatorio) o si el usuario puede elegir qué mensajes cifrar a la hora de enviarlos (Permitir). Este ajuste se aplica únicamente si se ha seleccionado el ajuste "Activar S/MIME". Valores posibles: • Obligatorio • Permitir El valor predeterminado es "Obligatorio".
Permitir Mail Drop	Esta configuración especifica si los usuarios pueden enviar archivos desde esta cuenta mediante Mail Drop.
VPN por cuenta	Esta configuración especifica el perfil de VPN que se utiliza para la comunicación de red de esta cuenta. Esta configuración se aplica únicamente a los dispositivos que ejecutan iOS 14 y posteriores o iPadOS 14 y posteriores.

Android: configuración del perfil de correo IMAP/POP3

Android: configuración del perfil de correo IMAP/POP3	Descripción
Prefijo de ruta IMAP	Si fuera necesario, esta configuración especifica el prefijo de la ruta de acceso de IMAP. Si fuera necesario, póngase en contacto con su ISP para obtener más información. Esta configuración solo es válida si el valor de la opción "Tipo de correo" se establece en "IMAP".

Android: configuración del perfil de correo IMAP/POP3	Descripción
Eliminar correo del servidor	Esta configuración especifica cuándo eliminar un correo desde el servidor de correo. Valores posibles: • Nunca • Al eliminarse de la bandeja de entrada El valor predeterminado es "Nunca". Esta configuración solo es válida si el valor de la opción "Tipo de correo" se establece en "POP3".

Windows: configuración del perfil de correo IMAP/POP3

Windows: configuración del perfil de correo IMAP/POP3	Descripción
Eliminar correo del servidor	En la configuración se especifica cómo se tratan los mensajes de correo cuando un usuario los elimina. Los mensajes de correo pueden eliminarse del servidor (eliminación permanente), o bien, de la bandeja de entrada pero conservarse en la carpeta de la papelera (eliminación temporal). Valores posibles: • Eliminación permanente • Eliminación temporal El valor predeterminado es "Eliminación temporal". Esta configuración solo es válida si el valor de "Tipo de correo" se establece como "IMAP".
Dominio	Esta configuración especifica el dominio del servidor de correo.
Intervalo de sincronización	Esta configuración especifica la frecuencia con que un dispositivo Windows descarga contenido nuevo del servidor de correo. Valores posibles: • Manual • 15 minutos • 30 minutos • 60 minutos • 2 horas El valor predeterminado es "15 minutos".

Windows: configuración del perfil de correo IMAP/POP3	Descripción
Cantidad de recuperación inicial	En la configuración se especifica el número de días transcurridos para sincronizar los mensajes de correo y los datos del organizador en un dispositivo Windows. Valores posibles: • Todas • 7 días • 14 días • 30 días El valor predeterminado es "7 días".
Usar solo la red móvil y no Wi-Fi	En la configuración se especifica si los mensajes de correo se envían y reciben solo a través de la red inalámbrica.

Configuración de los perfiles de CardDAV y CalDAV para los dispositivos con iOS y macOS

Puede utilizar perfiles de CardDAV y CalDAV para permitir que los dispositivos con iOS, iPadOS y macOS accedan a la información del calendario y a los contactos en un servidor remoto. Se pueden asignar perfiles de CardDAV y CalDAV a cuentas de usuarios, a grupos de usuarios y a grupos de dispositivos. Varios dispositivos pueden acceder a la misma información.

macOS aplica perfiles a las cuentas de usuario o los dispositivos. Los perfiles de CardDAV y CalDAV se aplican a cuentas de usuario.

Creación de un perfil de CardDAV

Antes de empezar:

- Compruebe que el dispositivo pueda acceder a un servidor CardDAV activo.

1. En la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Correo, Calendario y contactos > CardDAV**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil.
5. Escriba la dirección del servidor para el perfil. Es el FQDN del equipo que aloja la aplicación Calendario.
6. En el campo **Nombre de usuario**, realice una de las siguientes acciones:
   - Si el perfil es para un usuario, escriba el nombre de usuario.
   - Si el perfil es para varios usuarios, escriba `%UserName%`.
7. Si es necesario, introduzca el puerto para el servidor CardDAV.
8. Si es necesario, seleccione la casilla de verificación **Utilizar SSL** e introduzca la URL para el servidor SSL.
9. Si es necesario, en el campo **VPN por cuenta**, seleccione el perfil de VPN que desee utilizar para la comunicación de red de esta cuenta.
10. Haga clic en **Agregar**.

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

Creación de un perfil de CalDAV

Antes de empezar:

- Compruebe que el dispositivo pueda acceder a un servidor CalDAV activo.

1. En la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Correo, Calendario y contactos > CalDAV**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil.
5. Escriba la dirección del servidor para el perfil. Es el FQDN del equipo que aloja la aplicación Calendario.
6. En el campo **Nombre de usuario**, realice una de las siguientes acciones:
   - Si el perfil es para un usuario, escriba el nombre de usuario.

- Si el perfil es para varios usuarios, escriba `%UserName%`.

7. Si es necesario, introduzca el puerto para el servidor CalDAV.
8. Si es necesario, seleccione la casilla de verificación **Utilizar SSL** e introduzca la URL para el servidor SSL.
9. Si es necesario, en el campo **VPN por cuenta**, seleccione el perfil de VPN que desee utilizar para la comunicación de red de esta cuenta.
10. Haga clic en **Agregar**.

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

Aviso legal

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

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

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

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

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

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

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

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

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

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

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

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

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

Publicado en Canadá