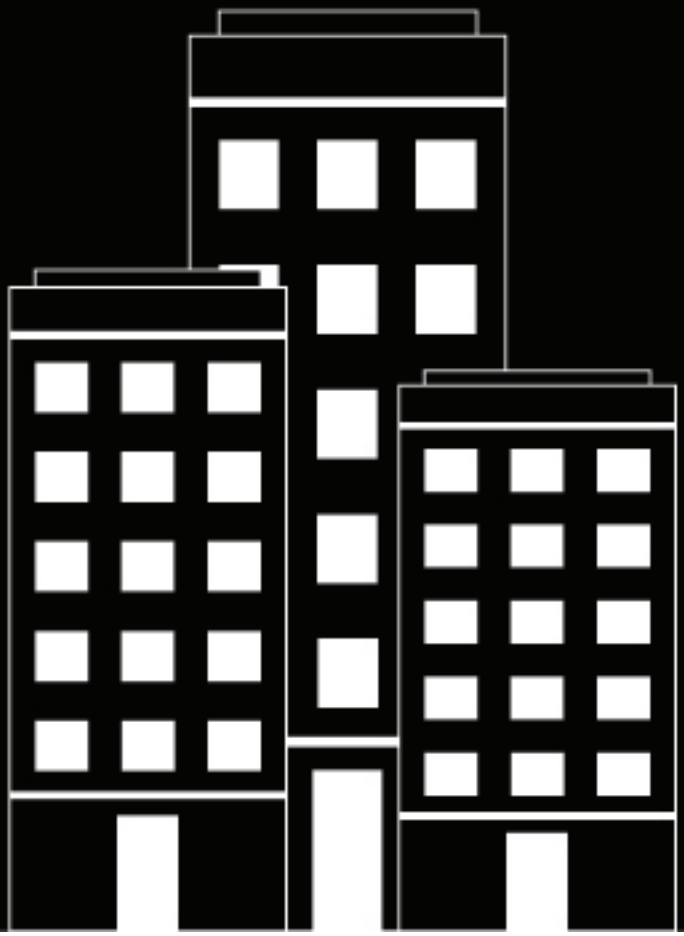

BlackBerry UEM

Administración

Gestión de administradores, usuarios y grupos

12.19

Contents

Gestión de administradores, usuarios y grupos de BlackBerry UEM

Esta guía proporciona instrucciones y detalles para crear y configurar cuentas de administrador, cuentas de usuario y grupos para administrar el entorno de BlackBerry UEM de su empresa.

Tarea	Descripción
Configurar las opciones de inicio de sesión para la consola de administración.	Configure el modo en que los administradores y los usuarios se autentican con las consolas UEM, incluida la complejidad de la contraseña, los avisos de inicio de sesión, los límites de tiempo de espera de la sesión y opciones como la autenticación basada en directorios y el registro único.
Creación y administración de roles de administrador.	Utilice roles de administrador preconfigurados o cree roles personalizados para configurar el nivel de control y los permisos que tienen los administradores en la consola de administración.
Creación de un administrador.	Cree usuarios administradores para administrar el entorno de UEM de su empresa.
Creación y administración de cuentas de usuario.	Cree cuentas de usuario directamente en UEM o cree cuentas de usuario desde el directorio de empresa de su organización.
Creación y administración de grupos de usuarios.	Cree grupos de usuarios para aplicar ajustes y configuraciones a varios usuarios.
Creación y administración de grupos de dispositivos.	Cree grupos de dispositivos para aplicar ajustes y configuraciones a tipos de dispositivos específicos.
Creación y administración de grupos de dispositivos compartidos.	Cree grupos de dispositivos compartidos para permitir que varios usuarios compartan un dispositivo iOS.
Creación y administración de grupos de dispositivos públicos.	Cree grupos de dispositivos públicos para administrar dispositivos de iOS de un solo propósito o dispositivos Android Enterprise que estén bloqueados para un conjunto específico de aplicaciones.
Creación y administración de grupos de iPad compartidos.	Cree grupos de iPad compartidos para permitir que varios usuarios inicien sesión y utilicen un dispositivo iPad compartido.
Administración de dispositivos Chrome OS.	Se utiliza UEM para realizar acciones de administración para los dispositivos Chrome OS.
Configuración de BlackBerry UEM Self-Service.	Permite que los usuarios accedan a UEM Self-Service para realizar tareas de administración de dispositivos por su cuenta.
Creación de roles de usuario para UEM Self-Service.	Utilice roles para administrar los permisos de usuario final para UEM Self-Service.

Tarea	Descripción
Personalización de la lista de usuarios.	Modifique la lista de cuentas de usuario en la consola de administración para adaptarla a sus necesidades.

Configuración de opciones de inicio de sesión en la consola

Puede configurar la forma en que los administradores y los usuarios se autentican con las consolas de BlackBerry UEM, incluida la complejidad de contraseña requerida, los avisos de inicio de sesión y los límites de tiempo de espera de la sesión.

Puede permitir que los administradores y los usuarios inicien sesión utilizando los siguientes métodos de autenticación:

Opción de autenticación	Descripción
Autenticación basada en contraseña local	Los administradores y los usuarios locales pueden autenticarse con un nombre de usuario y una contraseña.
Autenticación basada en directorio	Si se conecta BlackBerry UEM al directorio de la empresa, los administradores y los usuarios pueden iniciar sesión con las credenciales de su directorio. Para obtener más información, consulte Conexión con los directorios de la empresa en el contenido de Configuración.
Registro único	Si conecta UEM a Microsoft Active Directory en un entorno local, puede configurar la autenticación de registro único para permitir a los administradores o a los usuarios omitir la página de inicio de sesión y acceder directamente a la consola de administración o a BlackBerry UEM Self-Service. No se requiere contraseña ni certificado para iniciar sesión. Consulte Configuración de registro único de BlackBerry UEM. UEM Cloud no es compatible con esta función.
Autenticación basada en certificados	Puede configurar la autenticación basada en certificados para que los administradores y los usuarios puedan iniciar sesión mediante un certificado de autenticación. Consulte Configurar la autenticación de consola basada en certificados. UEM Cloud no es compatible con esta función.
Autenticación de BlackBerry 2FA	Puede configurar la autenticación de BlackBerry 2FA para que los administradores y los usuarios puedan iniciar sesión mediante la autenticación de dos factores. Para obtener más información, consulte KB 73371. Esta función no es compatible en un entorno local.
Autenticación de BlackBerry Online Account	Puede establecer una autenticación de BlackBerry Online Account para que los administradores puedan iniciar sesión utilizando sus credenciales de BlackBerry Online Account. Esta función no es compatible en un entorno local.

Configure la complejidad mínima de la contraseña para administradores locales

Puede establecer los requisitos de longitud y complejidad mínimos de la contraseña para las cuentas de administrador local. Esta configuración surte efecto cuando los administradores cambian su contraseña de la cuenta.

1. En la barra de menús de la consola de administración, haga clic en **Configuración > Configuración general > Consola**.
2. En el campo **Número mínimo de caracteres**, introduzca la cantidad mínima de caracteres que debe tener una contraseña de la consola.
3. En el campo **Complejidad mínima de la contraseña**, seleccione la complejidad mínima para una contraseña de la consola.
4. Haga clic en **Guardar**.

Creación de un aviso de inicio de sesión para las consolas

Puede crear un aviso de inicio de sesión para que se muestre a los administradores o a los usuarios en un entorno local cuando accedan a la consola de administración de BlackBerry UEM o a BlackBerry UEM Self-Service. El aviso informa a los administradores o usuarios acerca de los términos y condiciones que deben aceptar para utilizar las consolas. UEM Cloud no es compatible con esta función.

1. En la barra de menús de la consola de administración, haga clic en **Configuración > Configuración general > Avisos de inicio de sesión**.
2. Haga clic en ✎.
3. Efectúe una de las acciones siguientes:

Tarea	Pasos
Configurar un aviso de inicio de sesión para la consola de administración de UEM.	**a.** Seleccione la casilla de verificación **Activar un aviso de inicio de sesión para la consola de administración**. **b.** Escriba la información que desea que se muestre a los administradores cuando inician sesión.
Configurar un aviso de inicio de sesión para UEM Self-Service.	**a.** Seleccione la casilla de verificación **Activar un aviso de inicio de sesión para la consola de autoservicio**. **b.** Escriba la información que desea que se muestre a los usuarios cuando inician sesión.

4. Haga clic en **Guardar**.

Establecimiento de los límites de tiempo de espera de la sesión

1. En la barra de menús de la consola de administración, haga clic en **Configuración > Configuración general > Consola**.
2. En el campo **Tiempo de espera de la sesión**, introduzca la cantidad de tiempo, en minutos, que transcurrirá antes de que finalice la sesión y se cierre la sesión del usuario.

3. En el campo **Advertencia de tiempo de espera de la sesión**, introduzca la cantidad de tiempo, en minutos, para mostrar la advertencia de tiempo de espera de la sesión antes de cerrar la sesión de un usuario.
4. Haga clic en **Guardar**.

Configuración de registro único de BlackBerry UEM

Si conecta BlackBerry UEM a Microsoft Active Directory, puede configurar la autenticación de registro único para permitir a los administradores o a los usuarios omitir la página de inicio de sesión y acceder directamente a la consola de administración o a BlackBerry UEM Self-Service. Cuando los administradores o los usuarios inician sesión en Windows, el navegador utiliza sus credenciales para autenticarlas con UEM automáticamente. La información de inicio de sesión de Windows puede incluir los credenciales de Active Directory o los credenciales derivados (por ejemplo, de lectores CAC o tokens digitales).

UEM Cloud no es compatible con esta función.

Antes de empezar:

- Para configurar la delegación restringida para la cuenta de Active Directory que UEM utiliza para la conexión de directorio, haga lo siguiente:
  1. Utilice la herramienta Editor ADSI de Windows Server o la herramienta de línea de comandos para agregar los siguientes SPN de UEM a la cuenta de Active Directory:
     HTTP/*<host_FQDN_or_pool_name>* (por ejemplo, HTTP/domain123.example.com)
     BASPLUGIN111/*<host_FQDN_or_pool_name>* (por ejemplo, BASPLUGIN111/domain123.example.com)
  2. En Microsoft Active Directory Users and Computers, en las propiedades de la cuenta de Microsoft Active Directory, en la pestaña **Delegación**, active **Confiar en este usuario para la delegación solo a los servicios especificados** y **Utilizar solo Kerberos**.
  3. Añada los SPN a la lista de servicios.
- Si activa el registro único para varias conexiones de Active Directory, verifique que no haya relaciones de confianza entre los bosques de Active Directory.

1. En la barra de menús de la consola de administración de UEM, haga clic en **Configuración > Integración externa > Directorio de empresa**.
2. En la sección **Conexiones de directorio configuradas**, haga clic en una conexión de Active Directory.
3. En la pestaña **Autenticación**, seleccione la casilla de verificación **Activar registro único de Windows**.
4. Haga clic en **Guardar**.
5. Vuelva a hacer clic en **Guardar**.
6. Haga clic en **Cerrar**.

Después de terminar:

- Reinicie los servicios de UEM en cada equipo que aloje una instancia de UEM.
- Indique a los administradores y usuarios que utilicen las siguientes URL:
  - Consola de administración: https://*<host_FQDN_or_pool_name>*:*<port>*/admin
  - UEM Self-Service: https://*<host_FQDN_or_pool_name>*:*<port>*/mydevice

  La autenticación de registro único tiene prioridad sobre otros métodos de autenticación. Si los estándares de seguridad de su organización requieren que los administradores o usuarios utilicen otro método de autenticación, el método de registro único se puede eludir añadiendo ?sso=n al final de las URL anteriores.
- Indique a los administradores y a los usuarios de UEM Self-Service que configuren los navegadores para que admitan el registro único de UEM:

- Microsoft Edge: la consola de administración y las direcciones URL de UEM Self-Service deben estar asignadas a la zona de intranet local. Active la autenticación integrada de Windows.
- Mozilla Firefox: en la lista about:config, https://, *<host_FQDN_or_pool_name>* se añade a la preferencia "network.negotiate-auth.trusted-uris".
- Google Chrome: la consola de administración y las direcciones URL de UEM Self-Service deben estar asignadas a la zona de intranet local.

Configurar la autenticación de consola basada en certificados

En un entorno local de BlackBerry UEM, puede configurar la autenticación basada en certificados para que los administradores puedan iniciar sesión mediante un certificado de autenticación. UEM verifica certificados comparándolos con el emisor, comprueba que el certificado sea válido mediante los ajustes de certificados OCSP o CRL y constata que el certificado coincida con un usuario en la base de datos de UEM. UEM Cloud no es compatible con esta función.

Antes de empezar: Obtenga copias de los certificados de CA que distribuyan los certificados de cliente de sus administradores y usuarios en formato .cer o .der.

1. En la barra de menús de la consola de administración, haga clic en **Configuración > Configuración general > Autenticación de la consola basada en certificados**.
2. Seleccione la casilla de verificación **Habilitar la autenticación basada en certificados**.
3. Haga clic en **Examinar** y navegue hasta los archivos de certificado de CA.

   UEM confía en todos los certificados emitidos por esta CA. Repita este paso para cargar más certificados.
4. Para obligar a UEM a verificar que el nombre principal de usuario del certificado coincida con un usuario de la base de datos de UEM, seleccione la casilla de verificación **Comprobar nombre principal de usuario para SAN**.

   Si el nombre principal de usuario del certificado coincide con un usuario conocido, UEM otorga acceso en función de los permisos del usuario.
5. Para obligar a UEM a verificar que la dirección de correo electrónico del usuario del certificado coincida con una dirección de correo electrónico de usuario de la base de datos de UEM, seleccione la casilla de verificación **Buscar dirección de correo electrónico**.

   Si la dirección de correo electrónico del usuario del certificado coincide con un usuario conocido, UEM otorga acceso en función de los permisos del usuario. Si selecciona **Buscar nombre principal de usuario para SAN** y **Buscar dirección de correo electrónico**, UEM busca el nombre principal de usuario antes de la dirección de correo electrónico y otorga acceso si coincide el nombre principal. Si en ninguna de las comprobaciones se encuentran coincidencias entre el certificado y un usuario conocido, UEM deniega el acceso.
6. Haga clic en **Guardar**.

Después de terminar: Si los usuarios acceden a UEM mediante Mozilla Firefox, el usuario debe añadir su certificado de cliente al almacén de certificados de Firefox para autenticarse con UEM mediante la autenticación basada en certificados.

Creación y gestión de funciones de administrador

Puede asignar roles preconfigurados a los administradores o puede crear roles personalizados para cumplir los requisitos de su empresa. Debe ser un administrador de seguridad para crear roles personalizados, ver información acerca de un rol, cambiar la configuración de los roles, clasificarlos y eliminarlos.

Permisos para roles de administrador preconfigurados

BlackBerry UEM incluye cuatro roles preconfigurados para administradores. El rol de administrador de seguridad tiene permisos totales, que incluyen la creación y gestión de roles y administradores. Este rol no se puede editar ni eliminar. Al menos un administrador debe tener asignado el rol de administrador de seguridad. El rol de administrador de empresa (todos los permisos excepto para crear y administrar roles y administradores), el rol principal del servicio de asistencia técnica (permisos para realizar tareas administrativas intermedias) y el rol secundario del servicio de asistencia técnica (permisos para realizar tareas administrativas básicas) se pueden editar o eliminar. Las siguientes tablas contienen una lista de los permisos que están activados de manera predeterminada para cada rol preconfigurado.

Algunos permisos solo se admiten en roles personalizados.

Funciones y administradores

Permiso	Administrador de seguridad	Administrador de la empresa	Administrador principal	Administrador secundario
Presentación de funciones	√	NOD	NOD	NOD
Creación y edición de funciones	√	NOD	NOD	NOD
Eliminación de funciones	√	NOD	NOD	NOD
Clasificación de funciones	√	NOD	NOD	NOD
Creación de administradores	√	NOD	NOD	NOD
Eliminación de administradores	√	NOD	NOD	NOD
Edición de atributos no administrativos de administradores	√	NOD	NOD	NOD
Cambio de la contraseña para otros administradores	√	NOD	NOD	NOD

Permiso	Administrador de seguridad	Administrador de la empresa	Administrador principal	Administrador secundario
Cambio de la pertenencia a la función para administradores	√	NOD	NOD	NOD

Acceso al directorio

Puede especificar los directorios de la empresa en los que el administrador puede buscar.

Permiso	Administrador de seguridad	Administrador de la empresa	Administrador principal	Administrador secundario
Todos los directorios de la empresa	√	√	√	√
Solo directorios seleccionados de la empresa				

Administración del grupo

Puede especificar los grupos que el administrador puede administrar. Para gestionar usuarios que no pertenecen a un grupo, los administradores deben tener permiso para administrar todos los grupos y usuarios.

Permiso	Administrador de seguridad	Administrador de la empresa	Administrador principal	Administrador secundario
Todos los grupos y usuarios	√	√	√	√
Grupos seleccionados				

Usuarios y dispositivos

Permiso	Administrador de seguridad	Administrador de la empresa	Administrador principal	Administrador secundario
Ver usuarios y dispositivos activados	√	√	√	√
Crear usuarios	√	√	√	
Editar usuarios	√	√	√	√
Asignar funciones de usuario	√	√	√	√

Permiso	Administrador de seguridad	Administrador de la empresa	Administrador principal	Administrador secundario
Eliminar usuarios	√	√	√	
Exportar lista de usuarios	√	√		
Generar contraseña de activación y enviar correo	√	√	√	√
Generar contraseñas de activación y enviar mensajes de correo electrónico de activación a varios usuarios	√	√	√	
Especificar una contraseña de activación	√	√	√	√
Especificar varias contraseñas de activación con perfiles de activación exclusivos para un usuario	√	√		
Especificar si las contraseñas de activación caducan después de la activación del primer dispositivo	√	√		
Ver claves de acceso y códigos QR de activación del usuario	√	√		
Especificar contraseña de la cuenta	√	√	√	√
Cambiar contraseñas de varias cuentas	√	√	√	
Establecer la autenticación previa BlackBerry 2FA	√	√		
Gestionar dispositivos	√	√	√	√

Permiso	Administrador de seguridad	Administrador de la empresa	Administrador principal	Administrador secundario
Activar espacio de trabajo	√	√	√	√
Desactivar espacio de trabajo	√	√	√	√
Bloquear espacio de trabajo	√	√	√	√
Restablecer contraseña del espacio de trabajo	√	√	√	√
Especificar contraseña de dispositivo	√	√	√	√
Bloquear dispositivo y establecer mensaje	√	√	√	√
Desbloquear dispositivo y borrar contraseña	√	√	√	√
Eliminar solo los datos de trabajo	√	√	√	√
Eliminar solo los datos de trabajo de varios dispositivos	√			
Eliminar todos los datos del dispositivo	√	√	√	√
Eliminar todos los datos del dispositivo de varios dispositivos	√			
Eliminar dispositivo	√	√		
Eliminar varios dispositivos	√			
Especificar contraseña de trabajo y bloquear	√	√	√	√
Obtener registros del dispositivo	√	√	√	

Permiso	Administrador de seguridad	Administrador de la empresa	Administrador principal	Administrador secundario
Activar bloqueo de activación	√	√	√	√
Desactivar bloqueo de activación	√	√	√	√
Modo perdido	√	√	√	√
Activar modo perdido	√	√	√	√
Desactivar modo perdido	√	√	√	√
Ubicar dispositivo	√	√	√	√
Inscribir dispositivo	√	√	√	
Reiniciar dispositivo	√	√	√	√
Actualizar software iOS	√	√	√	√
Actualizar el software iOS en varios dispositivos	√			
Desactivar dispositivo	√	√	√	√
Ver detalles de ubicación de dispositivo	√	√	√	
Ver historial de ubicaciones de dispositivo	√	√		
Ver información de enlace de Exchange	√	√		
Ver información de dispositivo DEP de Apple	√	√	√	√
Asignar configuraciones de inscripción	√	√		

Permiso	Administrador de seguridad	Administrador de la empresa	Administrador principal	Administrador secundario
Ver identificadores de contraseñas de un solo uso	√	√	√	√
Asignar identificadores de contraseñas de un solo uso	√	√		
Enviar correo a usuarios	√	√	√	
Ver historial de omisiones del bloqueo de activación	√	√	√	
Gestión de aplicaciones BlackBerry Dynamics	√	√	√	√
Bloquear aplicación	√	√	√	
Desbloquear aplicación	√	√	√	√
Eliminar datos de la aplicación	√	√	√	√
Controlar el registro de la aplicación	√	√	√	
Gestión de aplicaciones Intune	√	√	√	

Dispositivo dedicado

Permiso	Administrador de seguridad	Administrador de la empresa	Administrador principal	Administrador secundario
Ver ajustes de grupo de dispositivos compartidos	√	√		
Crear y editar grupos de dispositivos compartidos	√	√		

Permiso	Administrador de seguridad	Administrador de la empresa	Administrador principal	Administrador secundario
Eliminar grupos de dispositivos compartidos	√	√		
Ver ajustes de grupo de dispositivos públicos	√	√		
Crear y editar grupos de dispositivos públicos	√	√		
Eliminar grupos de dispositivos públicos	√	√		

Grupos

Permiso	Administrador de seguridad	Administrador de la empresa	Administrador principal	Administrador secundario
Ver ajustes de grupo	√	√	√	√
Crear y editar grupos de usuarios	√	√	√	
Asignar funciones de usuario	√	√	√	
Agregar y eliminar usuarios de los grupos de usuarios	√	√	√	
Eliminar grupos de usuarios	√	√		
Crear y editar grupos de dispositivos	√	√	√	
Eliminar grupos de dispositivos	√	√		

Políticas y perfiles

Permiso	Administrador de seguridad	Administrador de la empresa	Administrador principal	Administrador secundario
Ver políticas de TI	√	√	√	√
Crear y editar políticas de TI	√	√		
Eliminar políticas de TI	√	√		
Ver perfiles de correo electrónico	√	√	√	√
Crear y editar perfiles de correo electrónico	√	√		
Eliminar perfiles de correo electrónico	√	√		
Ver perfiles de correo electrónico IMAP/POP3	√	√	√	√
Crear y editar perfiles de correo electrónico IMAP/POP3	√	√		
Eliminar perfiles de correo electrónico IMAP/POP3	√	√		
Ver perfiles de conectividad de empresa	√	√	√	√
Crear y editar perfiles de conectividad de empresa	√	√		
Eliminar perfiles de conectividad de empresa	√	√		
Ver perfiles de requisitos de solicitud de servicio del dispositivo	√	√	√	√

Permiso	Administrador de seguridad	Administrador de la empresa	Administrador principal	Administrador secundario
Crear y editar perfiles de requisitos de solicitud de servicio del dispositivo	√	√		
Eliminar perfiles de requisitos de solicitud de servicio del dispositivo	√	√		
Ver perfiles de activación	√	√	√	√
Crear y editar perfiles de activación	√	√		
Eliminar perfiles de activación	√	√		
Ver perfiles Wi-Fi	√	√	√	√
Crear y editar perfiles Wi-Fi	√	√		
Eliminar perfiles Wi-Fi	√	√		
Ver perfiles VPN	√	√	√	√
Crear y editar perfiles VPN	√	√		
Eliminar perfiles VPN	√	√		
Ver perfiles de conformidad	√	√	√	√
Crear y editar perfiles de conformidad	√	√		
Eliminar perfiles de conformidad	√	√		
Ver perfiles de dispositivo	√	√	√	√
Crear y editar perfiles de dispositivo	√			

Permiso	Administrador de seguridad	Administrador de la empresa	Administrador principal	Administrador secundario
Eliminar perfiles de dispositivo	√	√		
Ver perfiles de proxy	√	√	√	√
Crear y editar perfiles de proxy	√	√		
Eliminar perfiles de proxy	√	√		
Ver perfiles de filtro de contenido web	√	√	√	√
Crear y editar perfiles de filtro de contenido web	√	√		
Eliminar perfiles de filtro de contenido web	√	√		
Ver perfiles FileVault	√	√	√	√
Crear y editar perfiles FileVault	√	√		
Eliminar perfiles FileVault	√	√		
Ver perfiles de servicios de ubicación	√	√	√	√
Crear y editar perfiles de servicios de ubicación	√	√		
Eliminar perfiles de servicios de ubicación	√	√		
Ver perfiles de modo de bloqueo de la aplicación	√	√	√	√
Crear y editar perfiles de modo de bloque de la aplicación	√	√		

Permiso	Administrador de seguridad	Administrador de la empresa	Administrador principal	Administrador secundario
Eliminar perfiles de modo de bloqueo de la aplicación	√	√		
Ver perfiles de registro único	√	√	√	√
Crear y editar perfiles de registro único	√	√		
Eliminar perfiles de registro único	√	√		
Ver perfiles de certificado de CA	√	√	√	√
Crear y editar perfiles de certificado de CA	√	√		
Eliminar perfiles de certificado de CA	√	√		
Ver perfiles de certificado compartido	√	√	√	√
Crear y editar perfiles de certificado compartido	√	√		
Eliminar perfiles de certificado compartido	√	√		
Ver perfiles SCEP	√	√	√	√
Crear y editar perfiles SCEP	√	√		
Eliminar perfiles SCEP	√	√		
Ver perfiles OCSP	√	√	√	√
Crear y editar perfiles OCSP	√	√		
Eliminar perfiles OCSP	√	√		
Ver perfiles de recuperación de certificados	√	√	√	√

Permiso	Administrador de seguridad	Administrador de la empresa	Administrador principal	Administrador secundario
Crear y editar perfiles de recuperación de certificados	√	√		
Eliminar perfiles de recuperación de certificados	√	√		
Ver perfiles CRL	√	√	√	√
Crear y editar perfiles CRL	√	√		
Eliminar perfiles CRL	√	√		
Ver perfiles de dominios gestionados	√	√	√	√
Crear y editar perfiles de dominios gestionados	√	√		
Eliminar perfiles de dominios gestionados	√	√		
Ver perfiles de credenciales de usuario	√	√	√	√
Crear y editar perfiles de credenciales de usuario	√	√		
Eliminar perfiles de credenciales de usuario	√	√		
Ver perfiles de carga personalizados	√	√	√	√
Crear y editar perfiles de carga personalizados	√	√		
Eliminar perfiles de carga personalizados	√	√		
Asignar políticas de TI y perfiles a usuarios	√	√	√	√

Permiso	Administrador de seguridad	Administrador de la empresa	Administrador principal	Administrador secundario
Asignar políticas de TI y perfiles a grupos de usuarios	√	√	√	√
Asignar políticas de TI y perfiles a grupos de dispositivos	√	√	√	√
Asignar políticas de TI y perfiles a grupos de dispositivos compartidos	√	√		
Asignar políticas de TI y perfiles a grupos de dispositivos públicos	√	√		
Clasificar políticas de TI y perfiles	√	√		
Ver perfiles CardDAV	√	√	√	√
Crear y editar perfiles CardDAV	√	√		
Eliminar perfiles CardDAV	√	√		
Ver perfiles del servidor de calendario CalDAV	√	√	√	√
Crear y editar perfiles del servidor de calendario CalDAV	√	√		
Eliminar perfiles del servidor de calendario CalDAV	√	√		
Ver perfiles AirPrint	√	√	√	√
Crear y editar perfiles AirPrint	√	√		
Eliminar perfiles AirPrint	√	√		

Permiso	Administrador de seguridad	Administrador de la empresa	Administrador principal	Administrador secundario
Ver perfiles de uso de red	√	√	√	√
Crear y editar perfiles de uso de red	√	√		
Eliminar perfiles de uso de red	√	√		
Ver perfiles AirPlay	√	√	√	√
Crear y editar perfiles AirPlay	√	√		
Eliminar perfiles AirPlay	√	√		
Ver perfiles Enterprise Management Agent	√	√	√	√
Crear y editar perfiles Enterprise Management Agent	√	√		
Eliminar perfiles Enterprise Management Agent	√	√		
Ver perfiles de conformidad de BlackBerry Dynamics	√	√	√	√
Eliminar perfiles de conformidad de BlackBerry Dynamics	√	√		
Ver perfiles BlackBerry Dynamics	√	√	√	√
Crear y editar perfiles BlackBerry Dynamics	√	√		
Eliminar perfiles BlackBerry Dynamics	√	√		
Ver perfiles de conectividad de BlackBerry Dynamics	√	√	√	√

Permiso	Administrador de seguridad	Administrador de la empresa	Administrador principal	Administrador secundario
Crear y editar perfiles de conectividad de BlackBerry Dynamics	√	√		
Eliminar perfiles de conectividad de BlackBerry Dynamics	√	√		
Ver perfiles de no molestar	√	√	√	√
Crear y editar perfiles de no molestar	√	√		
Eliminar perfiles de no molestar	√	√		
Ver perfiles BlackBerry 2FA	√	√	√	√
Crear y editar perfiles BlackBerry 2FA	√	√		
Eliminar perfiles BlackBerry 2FA	√	√		
Ver perfiles de Windows Information Protection	√	√	√	√
Crear y editar perfiles de Windows Information Protection	√	√		
Eliminar perfiles de Windows Information Protection	√	√		
Ver perfiles de notificación por aplicación	√	√	√	√
Crear y editar perfiles de notificación por aplicación	√	√		
Eliminar perfiles de notificación por aplicación	√	√		

Permiso	Administrador de seguridad	Administrador de la empresa	Administrador principal	Administrador secundario
Ver perfiles de enlace	√	√	√	√
Crear y editar perfiles de enlace	√	√		
Eliminar perfiles de enlace	√	√		
Ver perfiles de protección de aplicaciones de Microsoft Intune	√	√	√	√
Crear y editar perfiles de protección de aplicaciones de Microsoft Intune	√	√		
Eliminar perfiles de protección de aplicaciones de Microsoft Intune	√	√		
Ver perfiles de diseño de la pantalla de inicio	√	√	√	√
Crear y editar perfiles de diseño de la pantalla de inicio	√	√		
Eliminar perfiles de diseño de la pantalla de inicio	√	√		
Ver política de autenticación de Enterprise Identity	√	√		
Crear y editar política de autenticación de Enterprise Identity	√	√		
Eliminar política de autenticación de Enterprise Identity	√	√		

Permiso	Administrador de seguridad	Administrador de la empresa	Administrador principal	Administrador secundario
Asignar política de autenticación de Enterprise Identity a usuarios y grupos	√	√		

Aplicaciones

Permiso	Administrador de seguridad	Administrador de la empresa	Administrador principal	Administrador secundario
Ver aplicaciones y grupos de aplicaciones	√	√	√	√
Crear y editar aplicaciones y grupos de aplicaciones	√	√		
Eliminar aplicaciones y grupos de aplicaciones	√	√		
Exportar datos de aplicación	√	√	√	√
Asignar aplicaciones y grupos de aplicaciones a usuarios	√	√	√	√
Asignar aplicaciones y grupos de aplicaciones a grupos de usuarios	√	√	√	√
Asignar aplicaciones y grupos de aplicaciones a grupos de dispositivos	√	√	√	√
Asignar aplicaciones y grupos de aplicaciones a grupos de dispositivos compartidos	√	√		
Asignar aplicaciones y grupos de aplicaciones a grupos de dispositivos públicos	√	√		

Permiso	Administrador de seguridad	Administrador de la empresa	Administrador principal	Administrador secundario
Editar configuración de clasificaciones y comentarios sobre la aplicación	√	√		
Eliminar clasificaciones y comentarios sobre la aplicación	√	√	√	√
Ver clasificación de instalación de aplicaciones	√	√	√	√
Editar clasificación de instalación de aplicaciones	√	√		
Ver licencias de aplicación	√	√	√	√
Crear licencias de aplicación	√	√		
Editar licencias de aplicación	√	√		
Eliminar licencias de aplicación	√	√		
Asignar licencias de aplicación a aplicaciones o grupos de aplicaciones	√	√	√	√

Aplicaciones restringidas

Permiso	Administrador de seguridad	Administrador de la empresa	Administrador principal	Administrador secundario
Ver aplicaciones restringidas	√	√	√	√
Crear aplicaciones restringidas	√	√		
Eliminar aplicaciones restringidas	√	√		

Aplicaciones personales

Permiso	Administrador de seguridad	Administrador de la empresa	Administrador principal	Administrador secundario
Ver aplicaciones personales	√	√		

Configuración de

Permiso	Administrador de seguridad	Administrador de la empresa	Administrador principal	Administrador secundario
Ver ajustes generales	√	√	√	√
Editar valores predeterminados de activación	√	√		
Crear y editar plantillas de correo electrónico	√	√		
Eliminar plantillas de correo electrónico	√	√		
Editar ajustes de la consola	√	√		
Editar idioma para correos automáticos	√	√		
Editar ajustes de la consola de autoservicio	√	√		
Crear copia de seguridad del espacio de trabajo y restablecer configuración[1]	√	√		
Eliminar copia de seguridad del espacio de trabajo y restablecer configuración[1]	√	√		
Editar variables predeterminadas[1]	√	√		

Permiso	Administrador de seguridad	Administrador de la empresa	Administrador principal	Administrador secundario
Editar avisos de inicio de sesión[1]	√	√		
Editar variables personalizadas	√	√		
Editar avisos de la organización	√	√		
Editar dominios de correo electrónico	√	√		
Editar ajustes del servicio de ubicación	√	√		
Editar configuración personalizada de la consola	√	√		
Editar configuración de caducidad del comando de eliminación	√	√		
Editar configuración de atestación	√	√		
Editar configuración del certificado	√	√		
Crear y editar notificaciones de eventos	√	√		
Eliminar notificaciones de eventos	√	√		
Editar mensajes de ayuda del dispositivo	√	√		
Editar configuración de autenticación basada en certificados[1]	√			
Editar configuración de acceso al servicio web público	√			

Permiso	Administrador de seguridad	Administrador de la empresa	Administrador principal	Administrador secundario
Ver gestión de la aplicación	√	√	√	√
Editar BlackBerry World para Work	√	√		
Editar almacenamiento de aplicaciones internas[1]	√	√		
Editar Work Apps de iOS	√	√		
Editar aplicaciones de Windows 10	√	√		
Editar configuración predeterminada de clasificaciones y comentarios sobre la aplicación	√	√		
Ver ajustes de integración externa	√	√	√	√
Editar configuración de Apple Push Notification	√	√		
Editar configuración del servidor SMTP[1]	√	√		
Edición de los ajustes de DEP de Apple	√	√		
Editar configuración del servidor BlackBerry 2FA	√	√		
Editar configuración de BlackBerry Connectivity Node[2]	√	√		
Ver identificadores de contraseñas de un solo uso	√	√	√	√

Permiso	Administrador de seguridad	Administrador de la empresa	Administrador principal	Administrador secundario
Crear y editar identificadores de contraseñas de un solo uso	√	√		
Editar ajustes del directorio de empresa	√	√		
Edición de la configuración de Microsoft Intune	√	√		
Edición de los ajustes de enlace de Microsoft Exchange	√	√		
Editar configuración de perfil de trabajo de Android	√	√		
Editar ajustes de la autoridad de certificación	√	√		
Editar configuración de inscripción masiva de Samsung Knox	√	√		
Ver certificados de confianza	√	√		
Agregar certificados de confianza	√	√		
Eliminar certificados de confianza	√	√		
Ver servidores de BlackBerry Connectivity Node	√	√		
Crear y editar servidores de BlackBerry Connectivity Node	√	√		
Eliminar servidores de BlackBerry Connectivity Node	√	√		

Permiso	Administrador de seguridad	Administrador de la empresa	Administrador principal	Administrador secundario
Ver configuración de BlackBerry Secure Gateway	√	√		
Edición de la configuración de BlackBerry Secure Gateway	√	√		
Ver usuarios y funciones de administrador	√	√	√	√
Ver resumen de licencias	√	√	√	√
Editar ajustes de licencias	√	√		
Ver ajustes de migración	√	√		
Editar ajustes de migración	√	√		
Ver ajustes de infraestructura	√	√	√	
Editar configuración de registro[1]	√	√		
Editar configuración de proxy del lado del servidor[1]	√	√		
Ver servidores[1]	√	√		
Editar servidores[1]	√	√		
Eliminar servidores[1]	√	√		
Administrar servidores[1]	√	√		
Ver ajustes de auditoría[1]	√	√		

Permiso	Administrador de seguridad	Administrador de la empresa	Administrador principal	Administrador secundario
Editar ajustes de auditoría y purgar datos[1]	√	√		
Ver configuración de BlackBerry Secure Connect Plus[1]	√	√		
Editar configuración de BlackBerry Secure Connect Plus[1]	√	√		
Ver certificados de servidor[1]	√	√		
Actualizar certificados de servidor[1]	√	√		
Ver configuración de BlackBerry Control	√	√	√	√
Edición de la configuración de BlackBerry Control	√	√		
Ver configuración de servidor proxy de BlackBerry Dynamics NOC[1]	√	√	√	√
Editar configuración de servidor proxy de BlackBerry Dynamics NOC[1]	√	√	√	√
Editar configuración de SNMP [1]	√	√		
Importar paquete de políticas de TI y metadatos de dispositivo[1]	√			
Ver configuración de servicios de colaboración[1]	√	√	√	√

Permiso	Administrador de seguridad	Administrador de la empresa	Administrador principal	Administrador secundario
Editar configuración de servicios de colaboración[1]	√	√		
Ver configuración de BlackBerry Dynamics	√	√	√	√
Ver servicios de aplicaciones de BlackBerry Dynamics	√	√		
Editar servicios de aplicaciones de BlackBerry Dynamics	√			
Crear servicios de aplicaciones de BlackBerry Dynamics	√			
Eliminar servicios de aplicaciones de BlackBerry Dynamics	√			
Ver propiedades de servidor de BlackBerry Dynamics[1]	√	√		
Editar propiedades de servidor de BlackBerry Dynamics[1]	√			
Ver configuración de BlackBerry Dynamics Direct Connect	√	√		
Edición de la configuración de BlackBerry Dynamics Direct Connect	√			
Ver configuración de clúster de servidor de BlackBerry Dynamics[1]	√	√		
Editar configuración de clúster de servidor de BlackBerry Dynamics[1]	√			

Permiso	Administrador de seguridad	Administrador de la empresa	Administrador principal	Administrador secundario
Ver informes de BlackBerry Dynamics	√	√	√	
Ver configuración de comunicación de BlackBerry Dynamics[1]	√	√	√	
Editar configuración de comunicación de BlackBerry Dynamics[1]	√			
Ver configuración de BEMS Mail[2]	√	√		
Editar configuración de BEMS Mail[2]	√			
Ver configuración de BEMS Docs[2]	√	√		
Editar configuración de BEMS Docs[2]	√			
Ver configuración de Enterprise Identity	√	√		
Ver configuración de empresa de Enterprise Identity	√	√		
Editar configuración de Enterprise Identity Enterprise	√	√		
Ver configuración de servicio de Enterprise Identity	√	√		
Editar configuración de servicio de Enterprise Identity	√	√		

[1] Solo entornos locales

[2] Solo entornos en la nube

Panel de control

Permiso	Administrador de seguridad	Administrador de la empresa	Administrador principal	Administrador secundario
Ver panel	√	√	√	√

Auditoría

Permiso	Administrador de seguridad	Administrador de la empresa	Administrador principal	Administrador secundario
Ver registros de auditoría del sistema[1]	√	√		
Ver registros de rendimiento del dispositivo[1]	√	√		

[1] Solo entornos locales

Espacios de trabajo

Permiso	Administrador de seguridad	Administrador de la empresa	Administrador principal	Administrador secundario
Administrador de organización	√			
Administrador de soporte técnico	√			
Administrador de soporte técnico de auditoría	√			

Creación de un rol de administrador personalizado

Si los roles de administrador preconfigurados no cumplen los requisitos de su organización, puede crear otros personalizados. También puede crear funciones personalizadas para restringir las tareas administrativas a una lista definida de grupos de usuarios. Por ejemplo, puede crear una función para administradores nuevos que restrinja sus permisos únicamente a un grupo de usuarios con fines de formación.

Antes de empezar:

- Debe ser un administrador de seguridad para crear una función personalizada.
- Revise el Permisos para roles de administrador preconfigurados.

1. En la barra de menús de la consola de administración, haga clic en **Configuración > Administradores > Funciones**.
2. Haga clic en .
3. Escriba un nombre y una descripción para la función.
4. Para copiar permisos de otro rol, haga clic en un rol de la lista desplegable **Permisos copiados del rol**.
5. Lleve a cabo una de estas acciones:

Tarea	Pasos
Permitir que los administradores con este rol busquen en todos los directorios de la empresa.	Seleccione la opción **Todos los directorios de la empresa**.
Permitir que los administradores con este rol busquen en los directorios de la empresa seleccionados.	a. Seleccione la opción **Solo directorios seleccionados de la empresa**. b. Haga clic en **Seleccionar directorios**. c. Seleccione uno o más directorios y haga clic en . d. Haga clic en **Guardar**.

6. Lleve a cabo una de estas acciones:

Tarea	Pasos
Permitir que los administradores con esta función gestionen todos los usuarios y grupos	Seleccione la opción **Todos los grupos y usuarios**.
Permitir que los administradores con esta función gestionen los grupos seleccionados	a. Seleccione la opción **Solo grupos seleccionados**. b. Haga clic en **Seleccionar grupos**. c. Seleccione uno o más grupos y haga clic en . d. Haga clic en **Guardar**.

7. Configure los permisos para los administradores de este rol.
8. Haga clic en **Guardar**.

Después de terminar: Para clasificar roles, cambiar su configuración o eliminarlos, consulte Gestión de funciones de administrador.

Gestión de funciones de administrador

Después de crear un rol de administrador, puede clasificar el rol, cambiar sus permisos o eliminarlo. BlackBerry UEM utiliza la clasificación para determinar qué rol se asigna a un administrador cuando este es miembro de varios grupos de usuarios que tienen roles diferentes. Si un rol se asigna directamente a una cuenta de usuario, tiene prioridad sobre los roles asignados a un grupo de usuarios. Si un administrador es miembro de varios grupos de usuarios que tienen funciones diferentes, UEM asigna la función con la clasificación más alta.

Antes de empezar: Para administrar roles de administrador, debe ser administrador de seguridad.

1. En la barra de menús de la consola de administración, haga clic en **Configuración > Administradores > Funciones**.
2. Lleve a cabo una de estas acciones:

Tarea	Pasos
Clasificar un rol.	**a.** Utilice las flechas para cambiar la clasificación del rol. **b.** Haga clic en **Guardar**.
Cambiar la configuración de un rol.	**a.** Haga clic en el nombre de la función que desea cambiar. **b.** Haga clic en **Editar**. **c.** Haga los cambios. **d.** Haga clic en **Guardar**.
Eliminar un rol.	**a.** Haga clic en el nombre de la función que desea eliminar. **b.** Haga clic en 🗑.

Creación de un administrador

Para crear un administrador, puede asignar un rol de administrador a una cuenta de usuario o a un grupo de usuarios. El grupo de usuarios puede ser un grupo vinculado a directorios o un grupo local. Puede añadir un rol a un usuario y un rol a cada grupo al que pertenece, pero BlackBerry UEM solo asigna un rol al usuario.

Cuando se asigna un rol a una cuenta de usuario o a un grupo de usuarios, UEM envía a los administradores un correo electrónico con su nombre de usuario y un enlace a la consola de administración. UEM también envía a los administradores un correo aparte con la contraseña de la consola de gestión. Si el administrador no tiene una contraseña de la cuenta, UEM genera una contraseña temporal y la envía al administrador.

Antes de empezar:

- Debe ser un administrador de seguridad para crear un administrador.
- Si es necesario, Creación de un rol de administrador personalizado.

1. En la barra de menús de la consola de administración, haga clic en **Configuración > Administradores**.
2. Lleve a cabo una de estas acciones:

Tarea	Pasos
Añadir un rol a una cuenta de usuario.	**a.** Haga clic en **Usuarios**. **b.** Haga clic en . **c.** Haga clic en el nombre de la cuenta de usuario a la que desea asignar el rol.
Asignar un rol a un grupo de usuarios.	**a.** Haga clic en **Grupos**. **b.** Haga clic en . **c.** Haga clic en el nombre del grupo de usuarios al que desea asignar el rol.

3. En la lista desplegable **Función**, haga clic en la función que desea asignar.
4. Haga clic en **Guardar**.

Después de terminar:

- Para cambiar un rol asignado, haga clic en el nombre de una cuenta de usuario o grupo de usuarios, haga clic en el rol que desea asignar y, a continuación, en **Guardar**.
- Para eliminar un administrador, seleccione la cuenta de usuario o el grupo de usuarios del que desea eliminar el rol y haga clic > **Eliminar**.

Creación y administración de cuentas de usuario

Puede crear cuentas de usuario directamente en BlackBerry UEM o, si se ha conectado UEM al directorio de la empresa, puede añadir cuentas de usuario desde el directorio de la empresa. También puede utilizar un archivo .csv para añadir varias cuentas de usuario a UEM al mismo tiempo.

Después de crear cuentas de usuario, puede habilitar servicios para los usuarios, añadir usuarios a grupos, activar los dispositivos de los usuarios en UEM y enviar comunicaciones a los usuarios.

Crear una cuenta de usuario

Antes de empezar:

- Si desea agregar un usuario de directorio, compruebe que BlackBerry UEM esté conectado al directorio de la empresa. Para obtener más información acerca de la conexión de UEM a un directorio de la empresa y de la activación de grupos vinculados a directorios, consulte Conexión a los directorios de la empresa en el contenido de Configuración.
- Si desea habilitar el servicio BlackBerry Workspaces para sus usuarios, verifique que el complemento Workspaces de UEM esté instalado en cada instancia de UEM de su entorno.

1. En la barra de menús de la consola de administración, haga clic en **Usuarios > Dispositivos gestionados > Añadir usuario**.
2. Lleve a cabo una de estas acciones:

Tarea	Pasos
Agregue un usuario de directorio.	**a.** En la pestaña **Directorio de la empresa**, busque el usuario de directorio que desea añadir. Puede buscar por nombre, apellidos, nombre para mostrar, nombre de usuario o dirección de correo. **b.** En los resultados de la búsqueda, seleccione la cuenta de usuario.
Agregue un usuario local.	**a.** En la pestaña **Local**, especifique el nombre y los apellidos del usuario. **b.** Opcionalmente, edite el nombre para mostrar del usuario. **c.** En el campo **Nombre de usuario**, escriba un nombre de usuario único. **d.** En el campo **Dirección de correo**, introduzca una dirección de correo de contacto para la cuenta de usuario. Se necesita una dirección de correo electrónico para la cuenta de usuario a fin de activar un servicio como, por ejemplo, Workspaces o la administración de dispositivos. **e.** También puede hacer clic en **Detalles adicionales del usuario** y rellenar los campos según corresponda.
Añada un usuario de BlackBerry Online Account (solo UEM Cloud).	**a.** En la pestaña **No directorio**, especifique el nombre y los apellidos del usuario. **b.** Opcionalmente, edite el nombre para mostrar del usuario. **c.** En el campo **Dirección de correo**, introduzca una dirección de correo de contacto para la cuenta de usuario. Se necesita una dirección de correo electrónico para la cuenta de usuario a fin de activar un servicio como, por ejemplo, Workspaces o la administración de dispositivos. **d.** También puede hacer clic en **Detalles adicionales del usuario** y rellenar los campos según corresponda.

3. Si existen grupos locales en UEM y desea añadir la cuenta de usuario a grupos, en la lista **Grupos disponibles**, haga clic en uno o más grupos y haga clic en ➔.

   Cuando se crea una cuenta de usuario, solo se puede añadir a grupos locales. Si la cuenta de usuario es miembro de un grupo vinculado a directorios, automáticamente se asocia con dicho grupo cuando se produce la sincronización entre UEM y el directorio de la empresa.
4. En un entorno en la nube, en **UEM Self-Service**, seleccione **BlackBerry Online Account** o **Cuenta de usuario de UEM local**. Si selecciona una cuenta de usuario de UEM local, cree una contraseña para BlackBerry UEM Self-Service. Si el usuario tiene asignada una función administrativa, también pueden usar la contraseña para acceder a la consola de gestión.
5. En un entorno local, si añade un usuario local, en el campo **Contraseña**, cree una contraseña para UEM Self-Service. Si el usuario tiene asignada una función administrativa, también pueden usar la contraseña para acceder a la consola de gestión.
6. En la sección **Servicios activados**, seleccione la casilla de verificación **Activar usuario para la administración de dispositivos**.
7. Si el complemento Workspaces de UEM está instalado en el dominio, para activar el servicio Workspaces, haga lo siguiente:
   a) En la sección **BlackBerry Workspaces**, seleccione la casilla de verificación **Activar BlackBerry Workspaces**. De forma predeterminada, los usuarios con el servicio Workspaces reciben la función de Visitante.
   b) Seleccione uno o más roles de usuario y haga clic en ➔.
8. Lleve a cabo una de estas acciones:

Tarea	Pasos
Pedir a los usuarios que activen los dispositivos con el perfil de activación actualmente asignado.	**a.** En la lista desplegable **Opción de activación**, seleccione **Activación del dispositivo predeterminada**. **b.** En la lista desplegable **Contraseña de activación**, seleccione si desea configurar la contraseña o generar automáticamente una contraseña. **c.** De manera opcional, puede cambiar la caducidad del periodo de activación. **d.** Si desea que la contraseña de activación sea válida solo para una activación de dispositivo, seleccione **El periodo de activación caduca después de la activación del primer dispositivo**. **e.** En la lista desplegable **Plantilla del correo de activación**, seleccione la plantilla que desea utilizar para el correo de activación.
Empareje una contraseña de activación con un perfil de activación específico.	**a.** En la lista desplegable **Opción de activación**, haga clic en **Activación del dispositivo con perfil de activación especificado**. **b.** En la lista desplegable **Perfil de activación**, seleccione el perfil de activación que desee emparejar con una contraseña. **c.** En la lista desplegable **Contraseña de activación**, seleccione si desea configurar la contraseña o generar automáticamente una contraseña. **d.** De manera opcional, puede cambiar la caducidad del periodo de activación. **e.** Si desea que la contraseña de activación sea válida solo para una activación de dispositivo, seleccione **El periodo de activación caduca después de la activación del primer dispositivo**. **f.** En la lista desplegable **Plantilla del correo de activación**, seleccione la plantilla que desea utilizar para el correo de activación.

Tarea	Pasos
Permitir a los usuarios activar solo aplicaciones de BlackBerry Dynamics.	**a.** En la lista desplegable **Opción de activación**, seleccione **Generación de clave de acceso de BlackBerry Dynamics**. **b.** En la lista desplegable **Número de claves de acceso que se van a generar**, seleccione el número de claves. Cada clave solo puede usarse una vez para activar una aplicación de BlackBerry Dynamics. **c.** Seleccione el número de días que desea que la clave de acceso siga siendo válida. **d.** En la lista desplegable **Plantilla del correo de activación**, seleccione la plantilla que desea utilizar para el correo de activación.
Añada el usuario a UEM solamente.	En la lista desplegable **Opción de activación**, seleccione **No establecer**.

9. Si utiliza variables personalizadas, amplíe **Variables personalizadas** y especifique los valores apropiados para las variables que se han definido.
10. Lleve a cabo una de estas acciones:
    - Para guardar la cuenta de usuario, haga clic en **Guardar**.
    - Para guardar la cuenta de usuario y crear otra, haga clic en **Guardar y crear nueva**.

Creación de cuentas de usuario desde un archivo .csv

Puede importar cuentas de usuario desde un archivo .csv a BlackBerry UEM para crear varias cuentas de usuario a la vez. Puede crear el archivo .csv manualmente utilizando un archivo .csv de muestra que puede descargar desde la consola de administración (**Usuarios > Todos los usuarios > Añadir usuario > Importar > Descargar archivo .csv de muestra**).

En función de sus necesidades, también puede especificar la pertenencia al grupo y los ajustes de activación de las cuentas de usuario; para ello, incluya las siguientes columnas en el archivo .csv:

Encabezado de columna	Descripción
Suscripción de grupo	Asigne uno o más grupos de usuarios a cada cuenta de usuario. Utilice un punto y coma (;) para separar varios grupos de usuarios. Si no se incluye la columna Pertenencia al grupo, al importar el archivo se le dará la opción de seleccionar el grupo al que desea que se añadan todas las cuentas de usuario importadas.
MDM (BlackBerry UEM)	Especifique si el usuario está activado para MDM. Para activar un usuario para MDM, escriba "Activado".
Contraseña de activación	Especifique la contraseña de activación. Este valor es necesario si el valor "Generación de la contraseña de activación" se establece en "manual".
Plantilla de activación	Especifique el nombre de la plantilla de correo de activación que desea enviar al usuario. Si no especifica un nombre, se utiliza la plantilla de correo de activación predeterminada.

Encabezado de columna	Descripción
Caducidad de la contraseña de activación	Especifique el tiempo, en segundos, durante el que es válida la contraseña antes de que caduque.
Generación de la contraseña de activación	Especifique una de estas opciones: • Automático: la contraseña de activación se crea automáticamente y se envía al usuario. (Predeterminado) • Manual: la contraseña de activación se establece en la columna "Contraseña de activación". • Ignorar: no se genera ninguna contraseña de activación.
Enviar correo de activación	Especifique una de estas opciones: • Verdadero: el correo electrónico de activación se envía al usuario. • Falso: el correo electrónico de activación no se envía al usuario. Si la "Generación de la contraseña de activación" se establece en "Automático", el correo de activación se envía al usuario independientemente del valor en esta columna. Si el valor "Generación de la contraseña de activación" es "Manual" y está vacío, el valor predeterminado será Verdadero. Si el valor "Generación de la contraseña de activación" es "Ignorar", el usuario no recibirá un correo electrónico de activación de autoservicio.
Tipo de usuario	Esta columna es obligatoria siempre que el archivo .csv incluya tanto cuentas de usuario locales como de directorio. Especifique una de estas opciones: • L: cuentas de usuarios locales • D: cuentas de usuario de directorio
UID del directorio	Esta columna es una alternativa a introducir la dirección de correo electrónico para las cuentas de usuario de directorio. De forma predeterminada, la dirección de correo electrónico se usa para validar las cuentas de usuario de directorio; sin embargo, puede especificar que se utilice el directorio UID en su lugar. Si la cuenta de usuario no se puede validar en el directorio UID, se informa de un error. Si incluye un valor de UID del directorio para uno de sus usuarios, el encabezado de columna debe incluir el UID del directorio y todas las filas del archivo .csv deben incluir un UID de directorio o tener un marcador de posición vacío (,) para la columna UID del directorio.

Adición de cuentas de usuario a UEM mediante un archivo .csv

Antes de empezar:

- Prepare el archivo .csv. Para obtener más información, consulte Creación de cuentas de usuario desde un archivo .csv.
- Si el archivo .csv contiene cuentas de usuario de directorio, compruebe que BlackBerry UEM esté conectado al directorio de la empresa.

1. En la consola de gestión de la barra de menú, haga clic en **Usuarios**.
2. En la pestaña **Todos los usuarios** o **Dispositivos gestionados**, haga clic en **Añadir usuario**.
3. En la pestaña **Importar**, haga clic en **Examinar** y desplácese hasta el archivo .csv.
4. Haga clic en **Cargar**.

5. Si el archivo .csv no utiliza la columna "Pertenencia al grupo" y desea añadir cuentas de usuario a grupos, en la lista **Grupos disponibles**, seleccione uno o más grupos y haga clic en ➡. Haga clic en **Siguiente**.

   Al importar el archivo .csv, todas las cuentas de usuario se añaden a los grupos locales que se seleccionan. Si una cuenta de usuario es miembro de un grupo vinculado a directorios, automáticamente se asocia a dicho grupo cuando se produce la sincronización entre UEM y el directorio la empresa.
6. Revise la lista de cuentas de usuario y realice una de las siguientes acciones:
   - Para corregir los errores de cualquier cuenta de usuario de directorio no válida, haga clic en **Cancelar**, corrija el archivo y vuelva a subirlo.
   - Para agregar las cuentas de usuario válidas, haga clic en **Importar**. Las cuentas de usuario de directorio no válidas se ignoran.

Active los servicios de un usuario

Si se ha activado BlackBerry UEM para uno o más servicios (por ejemplo, Workspaces, BBM Enterprise o Enterprise Identity), puede activar un servicio para un usuario.

1. En la barra de menús de la consola de administración, haga clic en **Usuarios > Todos los usuarios**.
2. Busque una cuenta de usuario y haga clic en ella.
3. En la página de detalles del usuario, los servicios disponibles se enumeran bajo el nombre del usuario.
4. Si un servicio no está activado actualmente, aparece con un icono +. Haga clic en + para añadir el servicio.
5. Configure el servicio según sea necesario y guarde los cambios.

Después de terminar: Si desea quitar un servicio de un usuario, haga clic en ⛔. Haga clic en ⛔ en el servicio que desea eliminar. Antes de poder eliminar los controles MDM, debe eliminar los dispositivos activados del usuario. Antes de poder eliminar el servicio de Enterprise Identity, debe eliminar todas las asignaciones de Enterprise Identity del usuario.

Agregar usuarios a los grupos de usuarios

Para obtener más información acerca de los grupos de usuarios, consulte Creación y administración de grupos de usuarios. Tenga en cuenta que no puede cambiar la pertenencia de un usuario a un grupo vinculado a directorios.

Antes de empezar: Para añadir un usuario que tiene asignado un rol de administrador a un grupo de usuarios, debe ser un administrador de seguridad.

1. En la barra de menús de la consola de administración, haga clic en **Usuarios > Dispositivos gestionados**.
2. Seleccione la casilla de verificación junto a los usuarios que desea agregar a los grupos de usuarios.
3. Haga clic en 👥.
4. En la lista **Grupos disponibles**, seleccione uno o más grupos y haga clic en ➡.
5. Haga clic en **Guardar**.

Después de terminar:

- Para cambiar a qué grupo de usuarios pertenece un usuario, haga clic en el nombre de la cuenta de usuario cuya pertenencia desea cambiar. Haga clic en ✎ y, en la sección **Pertenencia al grupo**, utilice las flechas izquierda y derecha para añadir el usuario a los grupos o eliminarlo de los grupos.

- Para eliminar varios usuarios de un grupo de usuarios, en la barra de menús, haga clic en **Grupos**. Haga clic en el grupo de usuarios del que desea eliminarlos usuarios. Seleccione los usuarios que desea eliminar y haga clic en .

Gestión de cuentas de usuario

Antes de empezar: Crear una cuenta de usuario.

1. En la barra de menús de la consola de administración, haga clic en **Usuarios > Dispositivos gestionados**.
2. Lleve a cabo una de estas acciones:
   - Para gestionar un usuario individual, busque una cuenta de usuario, haga clic en ella y vaya al paso siguiente.
   - Para realizar una acción para varias cuentas de usuario a la vez, seleccione la casilla de verificación situada junto a cada cuenta de usuario que desee gestionar. Haga clic en una acción encima de la lista de usuarios (por ejemplo, puede añadir las cuentas de usuario seleccionadas a grupos de usuarios) y siga las instrucciones que aparecen en pantalla.
3. Efectúe una de las acciones siguientes:

Tarea	Pasos
Editar la información de un usuario.	**a.** Haga clic en . **b.** Realizar cambios en la cuenta de un usuario. **c.** Haga clic en **Guardar**.
Añadir una nota a la cuenta de un usuario.	**a.** Haga clic en . **b.** Escribir sus notas. Las notas que escriba se guardan y almacenan automáticamente en la cuenta de usuario, no en un dispositivo concreto.
Asigne una política de TI, un perfil, una aplicación o un grupo de aplicaciones al usuario.	**a.** En la sección correspondiente, haga clic en . **b.** Seleccione la política de TI, el perfil, la aplicación o el grupo de aplicaciones que desea asignar. Siga las indicaciones y seleccione la configuración adecuada para completar la asignación. **c.** Para eliminar una política de TI, un perfil, una aplicación o un grupo de aplicaciones del usuario, junto a la propiedad que desee eliminar, haga clic en .
Sincronización de la información del usuario del directorio	Haga clic en .
Eliminar una cuenta de usuario.	**a.** Haga clic en . **b.** Haga clic en **Eliminar**.

Envío de comunicaciones a los usuarios

Puede enviar un correo electrónico, incluido un mensaje de correo electrónico que contenga una contraseña de BlackBerry UEM Self-Service, a uno o más usuarios. Cuando se envía una contraseña, las contraseñas se generan aleatoriamente y se envía un mensaje de correo que contiene una contraseña a cada usuario. En un entorno local

de UEM, puede configurar la dirección de correo electrónico desde la que se envía el correo en la configuración del servidor SMTP.

Antes de empezar: Los usuarios a los que envíe el mensaje de correo electrónico deben tener una dirección de correo electrónico asociada a su cuenta de usuario.

1. En la barra de menús de la consola de administración, haga clic en **Usuarios > Dispositivos gestionados**.
2. Seleccione la casilla de verificación situada junto a cada usuario al que desee enviar el mensaje.
3. Lleve a cabo una de estas acciones:

Tarea	Pasos
Enviar un correo electrónico a los usuarios.	**a.** Haga clic en . **b.** Opcionalmente, para enviar una copia del correo electrónico a sí mismo o a otras personas, haga clic en **CC** y escriba una o más direcciones de correo electrónico. Separe las direcciones con comas o puntos y coma.
Enviar una contraseña de BlackBerry UEM Self-Service a los usuarios.	**a.** Haga clic en  . **b.** Haga clic en **Continuar**.

Creación y administración de grupos de usuarios

Un grupo de usuarios es un conjunto de usuarios relacionados que comparten propiedades comunes. La administración de usuarios como un grupo es más eficaz que la administración individual, ya que las propiedades de los usuarios se pueden agregar, modificar o eliminar para todos los miembros del grupo al mismo tiempo. Los usuarios pueden pertenecer a más de un grupo a la vez. Al crear y administrar un grupo de usuarios, puede asignar políticas de TI, perfiles y aplicaciones en la consola de administración. También puede definir un grupo como miembro de otro grupo.

Puede crear dos tipos de grupos de usuarios:

- Grupos vinculados a directorios: estos grupos se vinculan a grupos del directorio de la empresa. Solo las cuentas de usuario del directorio pueden ser miembros de un grupo vinculado al directorio.
- Grupos locales: estos grupos se crean y se mantienen en BlackBerry UEM y pueden tener asignadas cuentas de usuario locales y cuentas de usuario del directorio.

Para los grupos vinculados a directorios, UEM sincroniza periódicamente la pertenencia del grupo con los grupos de directorios de la empresa asociados. Los usuarios que se han añadido o eliminado del grupo de directorios de la empresa se añaden o se eliminan del grupo vinculado a directorios. Cuando los usuarios se añaden a un grupo de directorios de la empresa que está vinculado a un grupo vinculado a directorios, se les asignan las propiedades que están asignadas al grupo. Cuando se eliminan usuarios del grupo vinculado a directorios, las propiedades se eliminan del usuario.

Cada grupo vinculado a directorios puede vincularse a un único directorio de la empresa. Por ejemplo, si UEM tiene dos conexiones de Microsoft Active Directory, (A y B), y crea un grupo vinculado a directorios que está vinculado a una conexión A, solo podrá vincularlo a grupos de directorios de la conexión A. Debe crear nuevos grupos vinculados a directorios para cualquier conexión de directorio.

Sincronizar grupos vinculados a directorios no agregan ni eliminan usuarios en UEM. Para permitir que UEM cree cuentas de usuario cuando se creen nuevos usuarios de directorios de la empresa, debe permitir la integración.

Creación de un grupo vinculado a directorios

Puede crear grupos de usuarios que se vinculen a grupos del directorio de su empresa. BlackBerry UEM sincroniza periódicamente la pertenencia de un grupo vinculado al directorio con sus grupos asociados del directorio de la empresa. Cuando se añade o elimina un usuario del directorio de la empresa, se añade o elimina del grupo vinculado al directorio. Los perfiles, políticas y aplicaciones que asigne al grupo vinculado al directorio se asignan a los usuarios de ese grupo. Cuando se elimina a usuarios del grupo, esas propiedades se eliminan.

Antes de empezar: Permitir los grupos vinculados al directorio.

1. En la barra de menús de la consola de administración, haga clic en **Grupos > Usuario**.
2. Haga clic en .
3. Escriba el nombre del grupo.
4. En la sección **Grupos vinculados al directorio**, haga lo siguiente:
   a) Haga clic en .
   b) Escriba el nombre o parte del nombre del grupo de directorios de la empresa al que quiera vincularse.
   c) Si tiene más de una conexión de directorio de la empresa, seleccione la conexión que desea buscar. Tras haber realizado esta selección, el grupo vinculado a directorios se asociará permanentemente a la conexión seleccionada.
   d) Haga clic en .
   e) Seleccione el grupo de directorios de la empresa.

f) Haga clic en **Agregar**.
g) Si es necesario, para permitir que la configuración del directorio controle el número de grupos anidados, seleccione la casilla de verificación **Vincular grupos anidados**. Para establecer un vínculo con todos los grupos anidados, deje la casilla de verificación sin seleccionar.
h) Repita estos pasos para vincular grupos adicionales.

5. Efectúe una de las acciones siguientes:

Tarea	Pasos
Asigne un rol de usuario al grupo vinculado al directorio.	**a.** En la sección **Función de usuario**, haga clic en +. **b.** En la lista desplegable, haga clic en el nombre de la función de usuario que desea asignar al grupo. **c.** Haga clic en **Agregar**.
Asigne una política o un perfil de TI al grupo vinculado al directorio.	**a.** En la sección **Política de TI y perfiles**, haga clic en +. **b.** Haga clic en **Política de TI** o en un tipo de perfil. **c.** En la lista desplegable, haga clic en el nombre de la política de TI o del perfil que desea asignar al grupo. **d.** Haga clic en **Asignar**.
Asigne una aplicación al grupo vinculado al directorio.	**a.** En la sección **Aplicaciones asignadas**, haga clic en +. **b.** Busque y seleccione la aplicación que desea asignar. **c.** Haga clic en **Siguiente**. **d.** En la lista desplegable **Disposición**, realice una de las acciones siguientes: • Para instalar la aplicación automáticamente en los dispositivos e impedir que los usuarios la desinstalen, seleccione **Obligatorio**. • Para exigir a los usuarios que instalen la aplicación e impedir que las aplicaciones VPP de Apple se actualicen automáticamente, seleccione **Obligatorio sin actualizaciones**. • Para permitir que los usuarios instalen y desinstalen la aplicación, seleccione **Opcional**. • Para permitir que los usuarios instalen y eliminen la aplicación e impedir que las aplicaciones VPP de Apple se actualicen automáticamente, seleccione **Opcional sin actualizaciones**. **e.** En los dispositivos iOS, para asignar los ajustes de VPN por aplicación a una aplicación o grupo de aplicaciones, en la lista desplegable **VPN por aplicación**, seleccione los ajustes que desea asociar a la aplicación o grupo de aplicaciones. **f.** Haga clic en **Asignar**.

6. Haga clic en **Agregar**.

Adición de un grupo de directorios de la empresa a un grupo vinculado a directorios

Antes de empezar: Creación de un grupo vinculado a directorios.

1. En la barra de menús de la consola de administración, haga clic en **Grupos > Usuario**.
2. Haga clic en el grupo vinculado a directorios.

3. En la pestaña **Configuración**, haga clic en .
4. En la sección **Grupos vinculados al directorio**, haga clic en +.
5. Busque y seleccione el grupo de directorios de la empresa que desea añadir a un grupo vinculado a directorios existente.
6. Haga clic en **Agregar**.
7. Si fuera necesario, seleccione **Vincular grupos anidados**.

Creación de un grupo local

Puede crear un grupo de usuarios local en BlackBerry UEM al que puede asignar políticas de TI, perfiles y aplicaciones. Cuando añada cuentas de usuario al grupo, las propiedades que asigne al grupo se asignarán a cada miembro del grupo. Puede añadir cuentas de usuario locales y cuentas de usuario de directorio a un grupo local.

1. En la barra de menús de la consola de administración, haga clic en **Grupos > Usuario**.
2. Haga clic en .
3. Escriba un nombre y una descripción para el grupo.
4. Efectúe una de las acciones siguientes:

Tarea	Pasos
Asigne un rol de usuario al grupo local.	a. En la sección **Función de usuario**, haga clic en +. b. En la lista desplegable, haga clic en el nombre de la función de usuario que desea asignar al grupo. c. Haga clic en **Agregar**.
Asigne una política o un perfil de TI al grupo local.	a. En la sección **Política de TI y perfiles**, haga clic en +. b. Haga clic en **Política de TI** o en un tipo de perfil. c. En la lista desplegable, haga clic en el nombre de la política de TI o del perfil que desea asignar al grupo. d. Haga clic en **Asignar**.

Tarea	Pasos
Asigne una aplicación a un grupo local.	**a.** En la sección **Aplicaciones asignadas**, haga clic en +. **b.** Busque la aplicación que desea asignar al grupo y selecciónela. **c.** Haga clic en **Siguiente**. **d.** En la lista desplegable **Disposición**, realice una de las acciones siguientes: • Para instalar la aplicación automáticamente en los dispositivos e impedir que los usuarios la desinstalen, seleccione **Obligatorio**. Esta opción no está disponible para las aplicaciones de BlackBerry. • Para exigir a los usuarios que instalen la aplicación e impedir que las aplicaciones VPP de Apple se actualicen automáticamente, seleccione **Obligatorio sin actualizaciones**. • Para permitir que los usuarios instalen y desinstalen la aplicación, seleccione **Opcional**. • Para permitir que los usuarios instalen y eliminen la aplicación e impedir que las aplicaciones VPP de Apple se actualicen automáticamente, seleccione **Opcional sin actualizaciones**. Si la misma aplicación se asigna a una cuenta de usuario y al grupo de usuarios al que pertenece el usuario, tiene prioridad la disposición de la aplicación asignada a la cuenta de usuario. **e.** En los dispositivos iOS, para asignar la configuración de VPN por aplicación a una aplicación o un grupo de aplicaciones, en la lista desplegable **VPN por aplicación**, seleccione la configuración que desea asociar con la aplicación o el grupo de aplicaciones. **f.** Si está disponible, para los dispositivos iOS y Android, seleccione una configuración de aplicación para asignarla a la aplicación. **g.** Si utiliza Android Enterprise y ha creado seguimientos de aplicaciones en la consola de Google Play, seleccione un seguimiento para asignarlo a la aplicación. **h.** Haga clic en **Asignar**.

5. Haga clic en **Agregar**.

Adición de grupos anidados a un grupo de usuarios

Cuando anida un grupo dentro de un grupo de usuarios, los miembros del grupo anidado heredarán las propiedades del grupo de usuarios. Cree y mantenga la estructura de anidamiento en BlackBerry UEM y podrá anidar tanto en grupos vinculados a directorios como en grupos locales dentro de cada tipo de grupo de usuarios. Al añadir un grupo anidado a un grupo de usuarios, también se añadirán los grupos a los que pertenece el grupo anidado.

1. En la barra de menús de la consola de administración, haga clic en **Grupos > Usuario**.
2. Busque el nombre de un grupo de usuarios y haga clic en él.
3. En la pestaña **Grupos anidados**, haga clic en +.
4. Seleccione uno o más grupos.
5. Haga clic en **Agregar**.

Después de terminar: Para eliminar grupos anidados asignados directamente a un grupo de usuarios, en **Grupos**, haga clic en el nombre del grupo de usuarios del que desea eliminar un grupo. En la pestaña **Grupos anidados**, haga clic en ✕ junto al grupo anidado que desea eliminar.

Administración de un grupo de usuarios

Antes de empezar: Creación de un grupo local o Creación de un grupo vinculado a directorios.

1. En la barra de menús de la consola de administración, haga clic en **Grupos > Usuario**.
2. Busque el grupo de usuarios que desea administrar y haga clic en él.
3. Efectúe una de las acciones siguientes:

Tarea	Pasos
Ver información acerca de un grupo de usuarios.	**a.** Para ver las cuentas de usuario asignadas al grupo, haga clic en **Usuarios**. **b.** Para ver los grupos anidados asignados al grupo, haga clic en **Grupos anidados**. **c.** Para ver los grupos de directorios vinculados (si están disponibles) o las propiedades asignadas del grupo, haga clic en **Configuración**.
Cambiar el nombre o la descripción de un grupo de usuarios.	**a.** Haga clic en ✎. **b.** Cambiar el nombre o la descripción del grupo de usuarios. **c.** Haga clic en **Guardar**.
Gestionar los roles, perfiles o aplicaciones asignados del grupo de usuarios.	**a.** Haga clic en la pestaña **Configuración**. **b.** Para asignar un rol, un perfil o una aplicación al grupo de usuarios, haga clic en + junto a la sección correspondiente. **c.** Para eliminar un rol, un perfil o una aplicación del grupo de usuarios, haga clic en ✕ junto a la propiedad que desee eliminar.
Eliminar un grupo de usuarios.	**a.** Haga clic en 🗑. **b.** Haga clic en **Eliminar**.

Creación y administración de grupos de dispositivos

Un grupo de dispositivos es un conjunto de dispositivos con atributos comunes, tales como el modelo y el fabricante, el tipo y la versión del SO, el proveedor de servicios y la propiedad. En función de los atributos que defina, BlackBerry UEM mueve automáticamente los dispositivos dentro o fuera del grupo de dispositivos.

Puede utilizar grupos de dispositivos para aplicar diferentes conjuntos de políticas, perfiles y aplicaciones a dispositivos específicos. Las propiedades que asigne a un grupo de dispositivos tienen prioridad sobre las asignadas a un usuario o grupo de usuarios. No puede asignar perfiles de activación ni certificados de usuario a grupos de dispositivos.

Creación de un grupo de dispositivos

1. En la barra de menús de la consola de administración, haga clic en **Grupos > Dispositivo**.
2. Haga clic en .
3. Escriba un nombre para el grupo de dispositivos.
4. Opcionalmente, en la sección **Ámbito de los grupos de usuarios**, seleccione los grupos de usuarios a los que se debe aplicar el grupo de dispositivos. Si no selecciona ninguno de los grupos de usuarios, el grupo de dispositivos se aplica a todos los dispositivos activados.
5. En la sección **Consulta de dispositivo**, en la primera lista desplegable, realice una de las siguientes acciones:
   - Si desea incluir dispositivos que coincidan con todos los atributos definidos, seleccione **Todos**.
   - Si desea incluir dispositivos que coincidan al menos con uno de los atributos definidos, seleccione **Cualquiera**.
6. En la sección **Consulta de dispositivo**, defina los parámetros para el grupo de dispositivos. Consulte Parámetros de grupos de dispositivos.
7. Haga clic en **Siguiente**.
8. Efectúe una de las acciones siguientes:

Tarea	Pasos
Asignar un perfil o una política de TI al grupo de dispositivos.	**a.** En la sección **Política de TI y perfiles**, haga clic en +. **b.** Haga clic en **Política de TI** o en un tipo de perfil. **c.** En la lista desplegable, haga clic en el nombre de la política de TI o del perfil que desea asignar al grupo. **d.** Haga clic en **Asignar**.

Tarea	Pasos
Asignar una aplicación o un grupo de aplicaciones al grupo de usuarios.	**a.** En la sección **Aplicaciones asignadas**, haga clic en +. **b.** Busque la aplicación que desea asignar al grupo y selecciónela. **c.** Haga clic en **Siguiente**. **d.** En la lista desplegable **Disposición**, realice una de las acciones siguientes: • Para aplicaciones de iOS y Android, para exigir a los usuarios que sigan las acciones definidas para las aplicaciones en el perfil de conformidad que tengan asignado, seleccione **Obligatorio**. • Para exigir a los usuarios que instalen la aplicación e impedir que las aplicaciones VPP de Apple se actualicen automáticamente, seleccione **Obligatorio sin actualizaciones**. • Para permitir que los usuarios instalen y desinstalen la aplicación, seleccione **Opcional**. Esta opción no está disponible para los grupos de aplicaciones que admiten Android Enterprise. • Para permitir que los usuarios instalen y eliminen la aplicación e impedir que las aplicaciones VPP de Apple se actualicen automáticamente, seleccione **Opcional sin actualizaciones**. **e.** En los dispositivos iOS, para asignar la configuración de VPN por aplicación a una aplicación o un grupo de aplicaciones, en la lista desplegable **VPN por aplicación**, seleccione la configuración que desea asociar con la aplicación o el grupo de aplicaciones. **f.** Si está disponible, para los dispositivos iOS y Android, seleccione una configuración de aplicación para asignarla a la aplicación. **g.** Si utiliza Android Enterprise y ha creado seguimientos de aplicaciones en la consola de Google Play, seleccione un seguimiento para asignarlo a la aplicación. **h.** Haga clic en **Asignar**. Tenga en cuenta que no puede añadir aplicaciones de BlackBerry Dynamics a grupos de dispositivos porque los derechos solo pueden concederse a los usuarios. Cualquier aplicación de BlackBerry Dynamics incluida en los grupos de aplicaciones que añada a los grupos de dispositivos no se asignará al usuario. Si su entorno es compatible con Android Enterprise, no puede añadir aplicaciones de Android que tengan una disposición opcional a grupos de dispositivos. Google Play for Work solo puede asignar aplicaciones a los ID de usuario de Google, no a los ID de dispositivo. Si agrega aplicaciones Android que tienen una disposición requerida a un grupo de dispositivos, las aplicaciones se instalarán, pero no se mostrarán en Google Play for Work.

9. Haga clic en **Guardar**.

Parámetros de grupos de dispositivos

Cuando se crea un grupo de dispositivos, se configura una consulta de dispositivo que incluye una o más instrucciones de atributo. Puede especificar si un dispositivo pertenece al grupo de dispositivos, si coincide con cualquier instrucción de atributo o solo si coincide con todas las instrucciones de atributo. Cada instrucción de atributo contiene un atributo, un operador y un valor.

Atributo	Operadores	Valores
Operador	• = • != • Comienza por	Especifique el nombre de un proveedor de servicios, como T-Mobile o Bell.
BlackBerry Dynamics	• = • !=	En la lista desplegable, seleccione una de las opciones siguientes: • Desactivado • Activado
Fabricante	• = • != • Comienza por	Especifique el nombre de un fabricante de dispositivos (por ejemplo, Apple).
Modelo	• = • != • Comienza por	Especifique el nombre de un modelo de dispositivo (por ejemplo, iPhone 15).
OS	• = • !=	En la lista desplegable, seleccione el sistema operativo adecuado.
Versión del SO	• = • != • >= • <=	Especifique la versión del sistema operativo (por ejemplo, 7.1.1 o 10.3). Si se utiliza este atributo, también deberá especificar el atributo del SO.
Propiedad	• = • !=	En la lista desplegable, seleccione una de las opciones siguientes: • Trabajo • Personal • No especificado
Tipo de activación	• = • !=	En la lista desplegable, seleccione un tipo de activación. La lista contiene los mismos tipos de activación que están disponibles para su asignación en los perfiles de activación.
Knox Workspace	• = • != • Comienza por	Especifique una versión de Samsung Knox Workspace (por ejemplo, 3.2.1).

Gestión de un grupo de dispositivos

Antes de empezar: Creación de un grupo de dispositivos.

1. En la barra de menús de la consola de administración, haga clic en **Grupos > Dispositivos**.
2. Busque el grupo de dispositivos que desea gestionar y haga clic en él.
3. Lleve a cabo una de estas acciones:

Tarea	Pasos
Ver información acerca de un grupo de dispositivos.	**a.** Para ver los dispositivos asignados al grupo de dispositivos, haga clic en la pestaña **Dispositivos**. **b.** Para ver los grupos de usuarios, las consultas de los dispositivos, las políticas de TI, los perfiles o las aplicaciones asignadas al grupo de dispositivos, haga clic en la pestaña **Configuración**.
Edite un grupo de dispositivos.	**a.** Haga clic en ✎. **b.** Haga los cambios. **c.** Haga clic en **Guardar**.
Eliminar un grupo de dispositivos.	**a.** Haga clic en 🗑. **b.** Haga clic en **Eliminar**.

Creación y gestión de grupos de dispositivos compartidos

Si desea permitir que varios usuarios compartan un dispositivo iOS, puede crear un grupo de dispositivos compartidos. Puede configurar los ajustes del grupo que sean específicos para cada usuario o los mismos para todos los usuarios. Al crear un grupo de dispositivos compartidos, BlackBerry UEM crea una cuenta de usuario local que es propietaria del grupo de dispositivos compartidos.

Para desproteger un dispositivo, los usuarios pueden utilizar la autenticación local o la de Microsoft Active Directory. Puede personalizar los términos de uso que los usuarios deben aceptar para desproteger dispositivos compartidos. Cuando se protege el dispositivo, está disponible para el siguiente usuario. Los dispositivos compartidos se gestionan mediante UEM durante el proceso de desprotección y protección.

Esta función se ha diseñado para dispositivos supervisados con la configuración siguiente:

- Modo de bloqueo de la aplicación activado
- Aplicaciones de VPP asignadas

Esta función no es compatible con aplicaciones de BlackBerry Dynamics. Se debe asignar el mismo perfil de BlackBerry Dynamics a la cuenta de usuario propietaria del grupo de dispositivos compartidos y también al grupo de dispositivos compartidos. Debe comprobar que la opción "Activar UEM Client para que pueda inscribirse en BlackBerry Dynamics" no esté seleccionada en el perfil.

Crear un grupo de dispositivos compartidos

Al crear un grupo de dispositivos compartidos, se crea una cuenta de usuario local. Esta cuenta de usuario local es la propietaria del grupo de dispositivos compartidos.

1. En la barra de menús de la consola de administración, haga clic en **Dispositivos dedicados > Grupos de dispositivos compartidos**.
2. Haga clic en +.
3. Escriba un nombre y una descripción para el grupo de dispositivos compartidos.
4. Escriba el nombre de usuario para la activación de los dispositivos.
5. Para solicitar a los usuarios que acepten los términos de servicio cuando marquen un dispositivo compartido, seleccione **Activar términos de servicio** y especifique los términos del servicio.
6. Para cada usuario que desee añadir al grupo, en la sección **Usuarios otorgados**, busque el usuario y haga clic en él.

   Los usuarios pueden pertenecer a varios grupos de dispositivos compartidos.
7. Para asignar una aplicación o un grupo de aplicaciones, en la sección **Aplicaciones asignadas**, haga clic en + y realice lo siguiente:
   a) Busque la aplicación que desea asignar al grupo y selecciónela.
   b) Haga clic en **Siguiente**.
   c) En el caso de las aplicaciones iOS o Android, para exigir a los usuarios que sigan las acciones definidas para las aplicaciones en el perfil de conformidad que se les ha asignado, en la lista desplegable **Disposición**, seleccione **Obligatorio**.

      Si el grupo de aplicaciones es compatible con Android Enterprise, la disposición solo se puede establecer como **Obligatoria**.
   d) Para permitir que los usuarios instalen y desinstalen la aplicación, en la lista desplegable **Disposición**, seleccione **Opcional**.

e) En los dispositivos iOS, para asignar la configuración de VPN por aplicación a una aplicación o un grupo de aplicaciones, en la lista desplegable **VPN por aplicación**, seleccione la configuración que desea asociar con la aplicación o el grupo de aplicaciones.
f) Si procede, para los dispositivos iOS y Android, seleccione la configuración de aplicaciones que desee asignar a la aplicación.
g) Si utiliza Android Enterprise y ha creado seguimientos de aplicaciones en la consola de Google Play, seleccione un seguimiento para asignarlo a la aplicación.
h) Haga clic en **Asignar**.

   No puede agregar aplicaciones de BlackBerry Dynamics a grupos de dispositivos porque los derechos solo pueden otorgarse a los usuarios. Cualquier aplicación de BlackBerry Dynamics incluida en los grupos de aplicaciones que agregue a los grupos de dispositivos no se asignará a los usuarios.

   Si su entorno es compatible con Android Enterprise, no puede añadir aplicaciones de Android que tengan una disposición opcional a grupos de dispositivos. Google Play for Work solo puede asignar aplicaciones a los ID de usuario de Google, no a los ID de dispositivo. Si agrega aplicaciones Android que tienen una disposición requerida a un grupo de dispositivos, las aplicaciones se instalarán, pero no se mostrarán en Google Play for Work.

8. Haga clic en **Guardar**.

Después de terminar:

- Activar un dispositivo compartido.
- Para realizar cambios en el grupo de dispositivos compartidos, consulte Gestión de un grupo de dispositivos compartidos.

Activar un dispositivo compartido

Para que los usuarios puedan desinscribir dispositivos compartidos, debe activarlos. El tipo de activación Privacidad de usuario: inscripción de usuario no es compatible.

Antes de empezar: Compruebe que el perfil de BlackBerry Dynamics asignado al grupo de dispositivos compartidos no tenga seleccionada la opción "Activar UEM Client para que pueda inscribirse en BlackBerry Dynamics". Compruebe que el mismo perfil también se ha asignado a la cuenta de usuario propietaria del grupo de dispositivos compartidos.

1. En la barra de menús de la consola de administración, haga clic en **Dispositivos dedicados > Grupos de dispositivos compartidos**.
2. Busque el nombre de un grupo de dispositivos compartidos y haga clic en él.
3. Para obtener la dirección del servidor y las credenciales de activación que utiliza para activar el dispositivo, haga clic en **Activación del dispositivo**.
4. Para activar el dispositivo, siga las instrucciones que aparecen en pantalla.

Después de terminar: Compruebe que el dispositivo activado se muestra en la sección **Dispositivos compartidos**. Para generar un nombre de dispositivo, BlackBerry UEM añade un número al nombre del grupo. Por ejemplo, si el nombre del grupo es Ejemplo, el primer dispositivo que active se denomina Ejemplo 01.

Gestión de un grupo de dispositivos compartidos

Antes de empezar: Crear un grupo de dispositivos compartidos.

1. En la barra de menús de la consola de administración, haga clic en **Dispositivos dedicados > Grupos de dispositivos compartidos**.

2. Busque el nombre del grupo de dispositivos compartidos que desea gestionar y haga clic en él.
3. Efectúe una de las acciones siguientes:

Tarea	Pasos
Mostrar solo la pantalla de inicio de sesión de BlackBerry UEM Client cuando el dispositivo está registrado.	**a.** Haga clic en ✎. **b.** Seleccione la casilla de verificación **Activar el bloqueo de la aplicación UEM Client**. **c.** Haga clic en **Guardar**.
Editar la suscripción de usuarios para un grupo de dispositivos compartidos.	**a.** Navegue a la sección **Usuarios otorgados**. **b.** Para añadir un usuario al grupo, busque el usuario y haga clic en su nombre. **c.** Para quitar un usuario del grupo, en la columna **Acción**, haga clic en ✕.
Asignar una política de TI o un perfil a un grupo de dispositivos compartidos.	Puede asignar una política de TI y perfiles a un grupo dado de dispositivos compartidos cuando un usuario inscriba el dispositivo o cancele la inscripción de este. Para que se aplique la misma política o perfil de TI, tanto si el dispositivo está protegido como si está desprotegido, puede asignarlo a ambos estados. Si la política o perfil de TI asignado es diferente para cada estado, se aplican la política y los perfiles adecuados cada vez que se inscriba o se cancele la inscripción del dispositivo. **a.** En la pestaña **Configuración registrada**, en la sección **Política y perfiles de TI asignados**, haga clic en +. **b.** Haga clic en **Políticas de TI** o en un tipo de perfil. **c.** En la lista desplegable, haga clic en el nombre de la política de TI o del perfil que desea asignar a los dispositivos cuando se cancela su inscripción. **d.** Haga clic en **Asignar** o **Sustituir**. **e.** En la pestaña **Configuración registrada**, repita los pasos para asignar una política de TI y perfiles que se apliquen a los dispositivos compartidos cuando se registran.

Tarea	Pasos
Asignar una aplicación a un grupo de dispositivos compartidos.	Puede asignar aplicaciones o grupos de aplicaciones a un grupo de dispositivos compartidos que esté disponible cuando un usuario inscriba el dispositivo o cancele la inscripción de este. Para que las aplicaciones permanezcan en el dispositivo en todo momento, puede asignarlas a ambos estados. Las aplicaciones asignadas que están disponibles únicamente en un estado se agregan o eliminan correctamente cada vez que el dispositivo se inscribe o cada vez que se cancela su inscripción. Antes de seguir los pasos que se indican a continuación, añada la aplicación a la lista de aplicaciones disponibles o cree grupos de aplicaciones. **a.** En la pestaña **Configuración registrada**, en la sección **Aplicaciones asignadas**, haga clic en +. **b.** Busque y seleccione la aplicación o el grupo de aplicaciones que desea asignar. **c.** Haga clic en **Siguiente**. **d.** Configure la disposición de la aplicación, la VPN por aplicación, la configuración de la aplicación y realice un seguimiento según sea necesario. **e.** Haga clic en **Siguiente**. **f.** Seleccione **Sí** si desea asignar una licencia a la aplicación y configurar los ajustes de licencia según sea necesario. Seleccione **No** si no desea asignar una licencia o no tiene una licencia que asignar a la aplicación. **g.** Haga clic en **Asignar**. Los usuarios deben seguir las instrucciones para inscribirse en el programa de compras por volumen (VPP) en los dispositivos de la empresa antes de poder instalar aplicaciones de prepago. Los usuarios deben completar esta tarea una vez. **h.** En la pestaña **Configuración registrada**, repita los pasos para asignar aplicaciones o grupos de aplicaciones que deben permanecer instaladas en el dispositivo cuando se registre el dispositivo.
Eliminar un dispositivo de un grupo de dispositivos compartidos.	**a.** En la sección **Dispositivos compartidos**, en la columna **Acción**, haga clic en ×. **b.** Haga clic en **Eliminar solo los datos de trabajo**.
Eliminar un grupo de dispositivos compartidos.	**a.** Elimine todos los dispositivos del grupo de dispositivos compartidos. **b.** Haga clic en 🗑. **c.** Haga clic en **Eliminar**.

Creación y administración de grupos de dispositivos públicos

Un dispositivo público es un dispositivo con un único fin que está limitado a un conjunto específico de aplicaciones para realizar dicho fin. Esta función es compatible con dispositivos iOS y Android Enterprise.

Se debe asignar un perfil de modo de bloqueo de la aplicación y un perfil de activación compatible a un grupo de dispositivos públicos. Para Android Enterprise, el tipo de activación debe ser Solo espacio de trabajo (dispositivo Android Enterprise totalmente gestionado). Para iOS, el dispositivo debe ser un dispositivo iOS supervisado con controles de MDM.

Creación de un grupo de dispositivos públicos

1. En la barra de menús de la consola de administración, haga clic en **Dispositivos dedicados > Grupos de dispositivos públicos**.
2. Haga clic en +.
3. Escriba un nombre y una descripción para el grupo de dispositivos públicos.
4. Escriba el nombre de usuario para la activación de los dispositivos.
5. Para asignar una aplicación o grupo de aplicaciones al grupo, en la sección **Aplicaciones asignadas**, haga clic en + y realice las siguientes acciones:
   a) Busque la aplicación que desea asignar al grupo y selecciónela.
   b) Haga clic en **Siguiente**.
   c) En el caso de las aplicaciones iOS o Android, para exigir a los usuarios que sigan las acciones definidas para las aplicaciones en el perfil de conformidad que se les ha asignado, en la lista desplegable **Disposición**, seleccione **Obligatorio**.

      Si el grupo de aplicaciones es compatible con Android Enterprise, la disposición debe ser **Obligatoria**.
   d) Para permitir que los usuarios instalen y desinstalen la aplicación, en la lista desplegable **Disposición**, seleccione **Opcional**.
   e) En los dispositivos iOS, para asignar la configuración de VPN por aplicación a una aplicación o un grupo de aplicaciones, en la lista desplegable **VPN por aplicación**, seleccione la configuración que desea asociar con la aplicación o el grupo de aplicaciones.
   f) Si procede, para los dispositivos iOS y Android, seleccione la configuración de aplicaciones que desee asignar a la aplicación.
   g) Si utiliza Android Enterprise y ha creado seguimientos de aplicaciones en la consola de Google Play, seleccione un seguimiento para asignarlo a la aplicación.
6. Haga clic en **Asignar**.

   No puede añadir aplicaciones de BlackBerry Dynamics a grupos de dispositivos porque los derechos solo pueden otorgarse a los usuarios. Cualquier aplicación de BlackBerry Dynamics incluida en los grupos de aplicaciones que agregue a los grupos de dispositivos no se asignará a los usuarios.

   Si admite Android Enterprise, no puede añadir aplicaciones Android que tengan una disposición opcional a los grupos de dispositivos. Google Play for Work solo puede asignar aplicaciones a los ID de usuario de Google, no a los ID de dispositivo. Si agrega aplicaciones Android que tienen una disposición requerida a un grupo de dispositivos, las aplicaciones se instalarán, pero no se mostrarán en Google Play for Work.
7. Haga clic en **Guardar**.

Después de terminar:

- Cree un perfil de modo de bloqueo de la aplicación y asígnelo al grupo de dispositivos públicos.

- Cree un perfil de activación y asígnelo al grupo de dispositivos públicos. El tipo de activación para Android Enterprise debe ser Solo espacio de trabajo (dispositivo con Android Enterprise totalmente gestionado). El tipo de activación para iOS debe ser un dispositivo con iOS supervisado con controles de MDM.
- Activación de un dispositivo público.
- Para eliminar un grupo de dispositivos públicos, seleccione la casilla de verificación situada junto al grupo que desea eliminar y haga clic en .

Activación de un dispositivo público

Antes de empezar: Creación de un grupo de dispositivos públicos.

1. En la barra de menús de la consola de administración, haga clic en **Dispositivos dedicados > Grupos de dispositivos públicos**.
2. Busque el nombre de un grupo de dispositivos públicos y haga clic en él.
3. Para obtener la dirección del servidor y las credenciales de activación que utiliza para activar el dispositivo, haga clic en **Activación del dispositivo**.
4. Para activar el dispositivo, siga las instrucciones que aparecen en pantalla.

Después de terminar: Compruebe que el dispositivo activado se muestra en la sección **Dispositivos públicos**. Para generar un nombre de dispositivo, BlackBerry UEM añade un número al nombre del grupo. Por ejemplo, si el nombre del grupo es Ejemplo, el primer dispositivo que active se denomina Ejemplo 01.

Gestión de un grupo de dispositivos públicos

Antes de empezar: Creación de un grupo de dispositivos públicos.

1. En la barra de menús de la consola de administración, haga clic en **Dispositivos dedicados > Grupos de dispositivos públicos**.
2. Busque un grupo de dispositivos públicos y haga clic en él.
3. Efectúe una de las acciones siguientes:

Tarea	Pasos
Asigne una política de TI, un perfil o una aplicación a un grupo de dispositivos públicos.	**a.** En la sección correspondiente, haga clic en +. **b.** Seleccione la política de TI, el perfil o la aplicación que desea asignar. Siga las indicaciones y seleccione la configuración adecuada para completar la asignación. **c.** Para eliminar una política de TI, un perfil o una aplicación, haga clic en ✕ junto a la propiedad que desea eliminar.
Elimine un dispositivo de un grupo de dispositivos públicos.	En la sección **Dispositivos públicos**, en la columna **Acción**, haga clic en para el dispositivo.

Creación y gestión de grupos de iPad compartidos

Al crear un grupo de iPad compartidos, los usuarios pueden iniciar sesión en un iPad compartido con su ID de Apple gestionado, lo que les permite utilizar aplicaciones y marcadores comunes al tiempo que mantienen y sincronizan detalles de usuario independientes.

Tenga en cuenta los siguientes requisitos:

- El dispositivo iPad debe ser un dispositivo supervisado inscrito en MDM.
- El dispositivo iPad debe estar inscrito en DEP.
- El dispositivo iPad debe utilizar una versión compatible de iPadOS.

Esta función no es compatible con aplicaciones de BlackBerry Dynamics. Debe comprobar que la opción "Activar UEM Client para que pueda inscribirse en BlackBerry Dynamics" no esté seleccionada en el perfil BlackBerry Dynamics.

Creación de un grupo de iPad compartidos

1. En la barra de menús de la consola de administración, haga clic en **Dispositivos dedicados > Grupos de iPad compartidos**.
2. Haga clic en +.
3. Escriba un nombre y una descripción para el grupo de iPad.
4. Escriba el nombre de usuario para la activación de los dispositivos.
5. Para asignar una aplicación o grupo de aplicaciones al grupo, en la sección **Aplicaciones asignadas**, haga clic en + y realice las siguientes acciones:
   a) Busque la aplicación que desea asignar al grupo y haga clic en ella.
   b) Haga clic en **Siguiente**.
   c) Para requerir que los usuarios sigan las acciones definidas para las aplicaciones en el perfil de conformidad que tienen asignado, seleccione **Obligatorio** u **Obligatorio sin actualizaciones** en la lista desplegable **Disposición**.
   d) Para asignar los ajustes de VPN por aplicación a un grupo, en la lista desplegable **VPN por aplicación** del grupo, seleccione los ajustes que desea asociar al grupo.
   e) Si estuviera disponible, seleccione la configuración de la aplicación que debe asignarse a la aplicación.
   f) Haga clic en **Asignar**.
6. Haga clic en **Guardar**.

Después de terminar:

- De forma opcional, Creación de un perfil de iPad compartido.
- Activación de un dispositivo iPad compartido.
- Para hacer cambios en un grupo de dispositivos iPad compartidos, consulte Gestión de un grupo de dispositivos de iPad compartidos.

Creación de un perfil de iPad compartido

Opcionalmente, puede crear y asignar un perfil de iPad compartido para configurar cómo pueden utilizar los usuarios un dispositivo iPad compartido.

Antes de empezar: Creación de un grupo de iPad compartidos.

1. En la barra de menús de la consola de administración, haga clic en **Políticas y perfiles > Política > iPad compartido**.
2. Haga clic en +.
3. Escriba un nombre y una descripción para el nuevo perfil compartido de iPad.
4. En el campo **Tamaño de la cuota**, especifique en MB el tamaño de la cuota para cada usuario en el dispositivo compartido. Esta configuración tiene prioridad sobre la configuración "Usuarios residentes".
5. En el campo **Usuarios residentes**, especifique el número de usuarios para los que se debe dividir el espacio restante del dispositivo.
6. Si desea que el dispositivo utilice únicamente el modo de invitado, seleccione la opción **Solo sesión temporal**.
7. En el campo **Tiempo de espera de sesión temporal**, especifique en segundos el tiempo de espera de una sesión temporal.
8. En el campo **Tiempo de espera de la sesión de usuario**, especifique en segundos el tiempo de espera de una sesión normal.
9. Haga clic en **Guardar**.

Después de terminar:

- Asigne el perfil a un grupo de iPad compartido.
- Activación de un dispositivo iPad compartido.

Activación de un dispositivo iPad compartido

Antes de empezar:

- Creación de un grupo de iPad compartidos. De forma opcional, Creación de un perfil de iPad compartido.
- Cree una configuración de DEP con la opción "Activar modo iPad compartido" seleccionada y asígnela a un dispositivo iPad de DEP activado.
- Borre el dispositivo iPad.
- Compruebe que el perfil de BlackBerry Dynamics asignado al grupo de dispositivos iPad compartidos no tenga seleccionada la opción **Activar UEM Client para que pueda inscribirse en BlackBerry Dynamics**. Compruebe que el mismo perfil también se ha asignado a la cuenta de usuario propietaria del grupo de dispositivos iPad compartidos.

1. En la barra de menús de la consola de administración, haga clic en **Dispositivos dedicados > Grupos de iPad compartidos**.
2. Busque el nombre de un grupo de dispositivos iPad compartidos y haga clic en él.
3. Para obtener las credenciales de activación que utiliza para activar el dispositivo, haga clic en **Activación del dispositivo**.
4. Para activar el dispositivo, siga las instrucciones de activación del dispositivo que aparecen en pantalla.

Después de terminar: Para eliminar un dispositivo de un grupo de dispositivos iPad compartidos, haga clic en el nombre del grupo del que desea eliminar el dispositivo. En la pantalla **Detalles del dispositivo**, haga clic en **Eliminar dispositivo** o en **Eliminar todos los datos del dispositivo**.

Gestión de un grupo de dispositivos de iPad compartidos

Antes de empezar: Creación de un grupo de iPad compartidos.

1. En la barra de menús de la consola de administración, haga clic en **Dispositivos dedicados > Grupos de iPad compartidos**.

2. Busque un grupo de iPad compartidos y haga clic en él.
3. Efectúe una de las acciones siguientes:

Tarea	Pasos
Asignar una política de TI o un perfil a un grupo de iPad compartidos.	a. En la sección **Política y perfiles de TI asignados**, haga clic en +. b. Haga clic en **Políticas de TI** o en un tipo de perfil. c. En la lista desplegable, haga clic en el nombre de la política de TI o del perfil que desea asignar. d. Haga clic en **Asignar** o **Sustituir**.
Asignar una aplicación a un grupo de iPad compartidos.	No puede añadir aplicaciones de BlackBerry Dynamics a grupos de iPad compartidos porque los derechos solo pueden otorgarse a los usuarios. Cualquier aplicación de BlackBerry Dynamics incluida en los grupos de aplicaciones que añada a los grupos de iPad compartidos no se asignará a los usuarios. Solo se admiten VPP de la tienda de aplicaciones o aplicaciones internas de iOS, así como accesos directos de aplicaciones de iOS. No se admiten aplicaciones de tiendas que no sean VPP. a. En la sección **Aplicaciones asignadas**, haga clic en +. b. Busque y seleccione la aplicación o el grupo de aplicaciones que desea asignar. c. Haga clic en **Siguiente**. d. Vuelva a hacer clic en **Siguiente**. e. Asigne una licencia de la aplicación VPP al dispositivo para cada aplicación. f. Haga clic en **Asignar**.

Gestión de dispositivos con Chrome OS en BlackBerry UEM

Puede integrar Chrome OS con la consola de administración de BlackBerry UEM para ampliar la capacidad para realizar algunas tareas administrativas en UEM. Continúa inscribiendo dispositivos Chrome OS y realizando algunas tareas administrativas en su consola de administración de Google. Cuando se integra Chrome OS con UEM, las unidades organizativas de la consola de administración de Google se ordenan en grupos de unidades organizativas de UEM. Cuando se realiza un cambio en una unidad organizativa, un usuario o un dispositivo en el dominio de Google, UEM actualiza su base de datos en consecuencia.

Para obtener más información acerca de la configuración de UEM para que sea compatible con los dispositivos Chrome OS, consulte Ampliación de la administración de dispositivos con Chrome OS a BlackBerry UEM.

Gestionar dispositivos con Chrome OS

Antes de empezar: Ampliación de la administración de dispositivos Chrome OS a BlackBerry UEM.

Efectúe una de las acciones siguientes:

Tarea	Pasos
Ver las unidades de organización para los usuarios de Chrome OS.	**a.** En la barra de menús de la consola de administración, haga clic en **Usuarios > Todos los usuarios**. **b.** Busque un usuario Chrome OS y haga clic en él. **c.** La unidad de organización a la que pertenece el usuario se muestra en la parte superior de la página. Puede hacer clic en el nombre de una unidad de organización para ver su configuración actual.
Editar una unidad de organización.	La información que se muestra para las unidades de organización replica lo que se ha configurado en la consola de administración de Google. Puede editar ciertos campos de una unidad de organización, pero muchos de los ajustes solo se pueden cambiar en la consola de administración de Google. **a.** En la barra de menús de la consola de administración, haga clic en **Grupos > Unidad de organización**. **b.** Haga clic en la unidad de organización que desea editar. **c.** Realice los cambios necesarios. **d.** Haga clic en **Guardar**.

Tarea	Pasos
Enviar comandos a dispositivos Chrome OS.	**a.** En la barra de menús de la consola de administración, haga clic en **Usuarios > Todos los usuarios**. **b.** Busque un usuario Chrome OS y haga clic en él. **c.** En la sección **Gestionar dispositivo**, haga clic en uno de los siguientes comandos: • Ver informe del dispositivo: este comando muestra información detallada sobre el dispositivo. • Ver acciones del dispositivo: este comando muestra todas las acciones que están en curso en el dispositivo. • Desactivar dispositivo: este comando desactiva el dispositivo. Tenga en cuenta que el usuario no puede volver a activar el dispositivo después de que un administrador lo haya desactivado. • Activar dispositivo: este comando activa el dispositivo. • Eliminar todos los datos del dispositivo: este comando elimina toda la información de usuario y los datos de aplicaciones y devuelve el dispositivo a la configuración predeterminada de fábrica. • Eliminar solo los datos de trabajo: este comando elimina los datos de trabajo y anula el aprovisionamiento del dispositivo. • Eliminar dispositivo: este comando anula el aprovisionamiento del dispositivo.

Configuración de BlackBerry UEM Self-Service

BlackBerry UEM Self-Service es una aplicación basada en web que permite a los usuarios de los dispositivos realizar tareas de administración, como crear contraseñas de activación, bloquear sus dispositivos de forma remota o eliminar datos de los mismos. Para utilizar UEM Self-Service, debe proporcionar la dirección web y la información de inicio de sesión a los usuarios.

1. En la barra de menús de la consola de administración, haga clic en **Configuración > Autoservicio > Configuración de autoservicio**.
2. Compruebe que la casilla de verificación **Permitir que los usuarios accedan a la consola de autoservicio** esté seleccionada.
3. Especifique cuánto tiempo tiene un usuario para activar un dispositivo antes de que caduque la contraseña de activación.
4. Especifique el número mínimo de caracteres requeridos en una contraseña de activación.
5. En la lista desplegable **Complejidad mínima de la contraseña**, seleccione el nivel de complejidad requerido para contraseñas de activación.
6. Para enviar automáticamente un correo electrónico de activación a los usuarios cuando crean una contraseña de activación en UEM Self-Service, seleccione la casilla de verificación **Enviar un correo electrónico de activación**. Puede utilizar la plantilla de correo de activación predeterminada o seleccionar una plantilla diferente en la lista desplegable.
7. Para enviar un correo electrónico de notificación de inicio de sesión al usuario cada vez que inicia sesión en UEM Self-Service, seleccione la casilla de verificación **Enviar notificación de inicio de sesión de autoservicio**.
8. Haga clic en **Guardar**.

Después de terminar:

- Proporcione la dirección web de BlackBerry UEM Self-Service y la información de inicio de sesión a los usuarios.
- Para crear y administrar roles de usuario para UEM Self-Service, consulte Administración de roles de usuario para BlackBerry UEM Self-Service.

Administración de roles de usuario para BlackBerry UEM Self-Service

Las funciones de usuario le permiten especificar las capacidades que están disponibles para los usuarios en BlackBerry UEM Self-Service. BlackBerry UEM Incluye una función de usuario predeterminada preconfigurada. El rol de usuario predeterminado está configurado para permitir todas las funciones de UEM Self-Service y se ha asignado al grupo "Todos los usuarios".

Nota: Al renombrar, eliminar o quitar la función de usuario predeterminada el grupo "Todos los usuarios", se pueden producir problemas con la aplicación Aplicaciones de trabajo en dispositivos iOS.

Si desea restringir determinadas funciones a los usuarios, puede crear nuevos roles de usuario o editar un rol de usuario existente. Puede asignar funciones de usuario a grupos o directamente a usuarios.

Solo se asigna una función a un usuario. Un rol asignado directamente a una cuenta de usuario tiene prioridad sobre un rol asignado indirectamente por un grupo de usuarios. Si un usuario es miembro de varios grupos de usuarios que tienen funciones de usuario diferentes, UEM asigna la función con la clasificación más alta.

Capacidades de BlackBerry UEM Self-Service

Función	Descripción
Especificar una contraseña de activación	Los usuarios pueden crear una contraseña que pueden utilizar para activar sus dispositivos con BlackBerry UEM. Puede configurar el período de caducidad y la complejidad de la contraseña predeterminada en **Configuración > Autoservicio > Configuración de autoservicio**.
Especificar clave de acceso	Los usuarios pueden crear claves de acceso que pueden utilizar para activar aplicaciones BlackBerry Dynamics.
Eliminar solo los datos de trabajo	Los usuarios pueden enviar el comando "Eliminar solo los datos de trabajo" a un dispositivo. El comando elimina los datos de trabajo, incluidos la política de TI, los perfiles, las aplicaciones y los certificados.
Eliminar todos los datos del dispositivo	Los usuarios pueden enviar el comando "Eliminar todos los datos del dispositivo" a un dispositivo. El comando elimina toda la información del usuario y los datos de las aplicaciones que guarda el dispositivo, incluida la información del espacio de trabajo. Devuelve el dispositivo a los valores predeterminados de fábrica y elimina el dispositivo de UEM.
Ubicar dispositivo	Los usuarios pueden ver la ubicación de sus dispositivos iOS o Android en un mapa. Esta función requiere que el usuario tenga asignado un perfil de servicio de ubicación. Para obtener más información, consulte Uso de los servicios de ubicación en los dispositivos.
Administrar certificados de usuario	Los usuarios pueden cargar certificados de usuario para sus dispositivos. Puede proporcionar instrucciones a los usuarios acerca de los certificados que necesitan y desde dónde deben cargarlos.

Función	Descripción
Bloqueo y desbloqueo de aplicaciones BlackBerry Dynamics	Si los dispositivos de los usuarios están habilitados para BlackBerry Dynamics, los usuarios pueden bloquear las aplicaciones de BlackBerry Dynamics instaladas en sus dispositivos y generar claves de desbloqueo para desbloquear las aplicaciones. Cuando un usuario bloquea una aplicación, nadie podrá abrirla.
Eliminar datos de aplicaciones BlackBerry Dynamics	Si los dispositivos de los usuarios están habilitados para BlackBerry Dynamics, los usuarios pueden eliminar todos los datos de una aplicación BlackBerry Dynamics instalada en un dispositivo. El comando elimina todos los datos almacenados por la aplicación, pero la aplicación no se elimina.

Creación de un rol de usuario para UEM Self-Service

Puede crear una función de usuario personalizada y asignarla a usuarios o grupos para especificar las capacidades que los usuarios tienen en BlackBerry UEM Self-Service.

1. En la barra de menús de la consola de administración, haga clic en **Configuración > Autoservicio > Funciones de usuario**.
2. Haga clic en .
3. Escriba un nombre y una descripción para la función de usuario.
4. Para copiar permisos de otro rol, haga clic en un rol de la lista desplegable **Permisos copiados del rol**.
5. Seleccione las capacidades que desea que tenga el rol de usuario.
6. Haga clic en **Guardar**.

Después de terminar:

- Clasifique los roles de usuario como corresponda y guarde los cambios.
- Asigne roles de usuario a grupos de usuarios (**Grupos > Busque un grupo y haga clic en él > Dispositivos gestionados**) o a usuarios individuales (**Usuarios > Dispositivos gestionados > Busque un usuario y haga clic en él > Asignación directa de funciones**).

Personalización de la lista de usuarios

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

Tarea	Pasos
Establezca la vista predeterminada o avanzada.	En la esquina superior derecha, haga clic en **Predeterminado** o **Avanzado**. En entornos de mayor tamaño, la vista avanzada puede tardar más tiempo en mostrarse que la vista predeterminada.
Seleccione la información que desea que aparezca en la lista de usuarios.	**a.** En la parte superior de la lista de usuarios, haga clic en  . **b.** Elegir las columnas que desea incluir o excluir. Para ordenar la lista de usuarios por una columna, haga clic en la cabecera de la columna. Para reorganizar las columnas, haga clic en la cabecera de una columna y arrástrela.
Filtrar la lista de usuarios.	Al activar la selección múltiple, puede seleccionar varios filtros antes de aplicarlos y también seleccionar varios filtros en cada categoría. Si la selección múltiple está desactivada, cada filtro se aplica cuando usted lo selecciona, y solo se puede seleccionar un filtro en cada categoría. **a.** Haga clic en para activar o desactivar la selección múltiple. **b.** En **Filtros**, amplíe una o más categorías. Cada categoría incluye solamente los filtros que muestran resultados y cada filtro indica el número de resultados que deben aparecer cuando se aplica. **c.** Seleccione los filtros que desea aplicar.
Exportar la lista de usuarios a un archivo .csv.	Al exportar la lista de usuarios, el archivo incluye todas las columnas que se muestran actualmente. **a.** Seleccione las cuentas de usuario que desea incluir en la exportación. Para seleccionar a todos los usuarios, puede seleccionar la casilla de verificación de la parte superior de la lista de usuarios. **b.** Haga clic en y guarde el archivo.

Tarea	Pasos
Cambiar la etiqueta de la propiedad de dispositivo.	Cada dispositivo activado tiene una etiqueta que indica si el dispositivo es propiedad de su empresa o del usuario, o si no se ha especificado. El valor predeterminado proviene de la configuración de propiedad del dispositivo en el perfil de activación. Puede filtrar la lista de usuarios por la etiqueta de propiedad del dispositivo. Siga los pasos que se indican a continuación para cambiar la etiqueta de propiedad del dispositivo para un usuario específico. Si desea cambiar la etiqueta para varios usuarios, puede enviar un comando masivo. **a.** Busque el nombre de una cuenta de usuario y haga clic en él. **b.** En la sección **Dispositivos activados**, junto a la configuración de propiedad, haga clic en **Editar**. **c.** Establezca la etiqueta de propiedad del dispositivo adecuada. **d.** Haga clic en **Guardar**.

Aviso legal

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

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

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

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

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

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

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

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

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

Publicado en Canadá