BlackBerry UEM

Administrar configuraciones de dispositivos

12.20

Contents

Gestión de configuraciones de dispositivos

Esta guía proporciona instrucciones para utilizar perfiles BlackBerry UEM, políticas de TI y otras características clave para configurar los dispositivos de trabajo para que satisfagan las necesidades y los requisitos de seguridad de su empresa.

Tarea	Descripción
Uso de perfiles para gestionar las funciones del dispositivo.	Configure y asigne perfiles de UEM a usuarios y grupos para administrar una amplia variedad de funciones y capacidades para todo tipo de dispositivos.
Uso de variables en perfiles, correos electrónicos y notificaciones.	Utilice variables en perfiles, notificaciones de cumplimiento, correos electrónicos de activación y notificaciones de eventos para personalizar configuraciones y mensajes para usuarios individuales.
Uso de plantillas de correo electrónico para enviar mensajes a los usuarios.	Utilice plantillas de correo electrónico para adaptar y personalizar los mensajes de correo electrónico que UEM envía a los usuarios por diversos motivos, como proporcionar instrucciones para la activación del dispositivo, notificar a los usuarios sobre problemas de conformidad y proporcionar claves de acceso para las aplicaciones de BlackBerry Dynamics.
Gestión de dispositivos con políticas de TI.	Utilice políticas de TI para controlar las características y la funcionalidad del dispositivo. Por ejemplo, puede utilizar reglas de política de TI para imponer requisitos de contraseña, impedir el uso de determinadas características del dispositivo (por ejemplo, la cámara) y controlar la disponibilidad de ciertas aplicaciones.
Creación de mensajes de compatibilidad de dispositivos para las funciones desactivadas en los dispositivos Android.	Mostrar un mensaje de asistencia en los dispositivos Android cuando una política de TI desactiva una función.
Cumplimiento de las reglas de los dispositivos.	Utilice perfiles de conformidad para animar a los usuarios a seguir los estándares de dispositivos de su empresa. Un perfil de conformidad define las condiciones del dispositivo que no son aceptables en su organización y especifica las acciones de cumplimiento que UEM debe llevar a cabo si el usuario no corrige los problemas de conformidad.
Envío de comandos a usuarios y dispositivos.	Puede enviar varios comandos para gestionar las cuentas y los dispositivos de los usuarios. Por ejemplo, puede enviar un comando para bloquear un dispositivo o eliminar todos los datos de trabajo de un dispositivo.
Control del modo en que se instalan las actualizaciones de software en los dispositivos.	Utilice los perfiles de requisitos SR del dispositivo para controlar cómo se instalan las actualizaciones de software en los dispositivos.

Tarea	Descripción
Configuración de cómo los dispositivos se ponen en contacto con UEM para actualizaciones de aplicaciones y configuraciones.	Utilice perfiles Enterprise Management Agent para configurar cómo los dispositivos se ponen en contacto con UEM para las actualizaciones de aplicaciones o de configuración.
Presentación de la información de la empresa en los dispositivos.	Utilice los avisos de la empresa y los perfiles de dispositivo para mostrar la información de la empresa en los dispositivos.
Uso de servicios de ubicación en los dispositivos.	Puede utilizar perfiles de servicio de ubicación para solicitar la ubicación de los dispositivos y ver las ubicaciones aproximadas en un mapa.
Habilitación del bloqueo de activación para un dispositivo iOS.	La función de bloqueo de activación de los dispositivos iOS permite a los usuarios proteger sus dispositivos en caso de pérdida o robo. Cuando la función está activada, el usuario debe confirmar el ID y la contraseña de Apple ID para desactivar Buscar mi iPhone, borrar el dispositivo o reactivar y utilizar el dispositivo.
Administración de las funciones de iOS mediante perfiles de carga personalizados.	Se pueden utilizar perfiles de carga personalizados para controlar las funciones de los dispositivos iOS que no están controladas por las políticas o perfiles actuales de UEM.
Configuración de la protección contra el restablecimiento de los datos de fábrica para dispositivos Android.	Utilice los perfiles de protección contra el restablecimiento de los datos de fábrica para controlar la función de protección contra el restablecimiento de los dispositivos Android Enterprise y Android Management de la empresa.
Configuración de atestaciones de dispositivos.	Envíe comprobaciones para probar la autenticidad y la integridad de los dispositivos Samsung Knox, Android, iOS y Windows 10.
Configuración de Windows Information Protection de para dispositivos Windows 10.	Utilice los perfiles de Windows Information Protection para proteger y gestionar los datos de trabajo en los dispositivos Windows 10.
Movimiento de dispositivos con iOS o macOS a un canal reforzado.	Cuando se activan dispositivos con iOS o macOS, de forma predeterminada se asignan a un canal de datos reforzado. Si tiene algún dispositivo iOS o macOS que actualmente no utilice un canal reforzado, puede exportar una lista con esos dispositivos y tomar medidas para moverlos a un canal reforzado.

Uso de perfiles para gestionar las funciones del dispositivo

BlackBerry UEM utiliza diferentes tipos de perfiles para administrar una amplia variedad de funciones y capacidades de los dispositivos iOS, macOS, Android y Windows. Configure un perfil para satisfacer las necesidades de su empresa y, a continuación, asígnelo a cuentas de usuario, grupos de usuarios y grupos de dispositivos para aplicar esa configuración a los dispositivos.

Para obtener una lista completa de los perfiles disponibles, consulte Perfiles de BlackBerry UEM.

Los perfiles pueden ser clasificados o no clasificados. Para los perfiles clasificados, UEM asignará un perfil de ese tipo a un dispositivo (por ejemplo, un perfil de conformidad). Si un perfil clasificado se asigna directamente a un usuario, tiene prioridad sobre cualquier perfil de ese tipo asignado a los grupos de usuarios a los que pertenece el usuario. Si un usuario pertenece a varios grupos de usuarios que tienen asignados diferentes perfiles de ese tipo, se utiliza la clasificación para determinar qué perfil se debe asignar. Si el dispositivo de un usuario pertenece a un grupo de dispositivos, el perfil asignado al grupo de dispositivos tiene prioridad sobre el mismo perfil de ese tipo que se asigna directamente al usuario. Si el dispositivo pertenece a varios grupos de dispositivos con diferentes perfiles de ese tipo, se utiliza la clasificación para determinar qué perfil se debe asignar.

Para los perfiles sin clasificar, se puede asignar más de un perfil de ese tipo a un dispositivo, ya sea desde la asignación directa a una cuenta de usuario o a través de la asignación de grupo (por ejemplo, a un dispositivo se le puede asignar más de un perfil Wi-Fi).

Para determinados tipos de perfiles, se debe asignar un perfil a los dispositivos. Si un perfil no se asigna a los usuarios directamente o a través de la pertenencia a grupos, UEM asigna un perfil predeterminado preconfigurado. UEM incluye un perfil de activación predeterminado, un perfil de conformidad predeterminado, un perfil de conectividad de la empresa predeterminado y un perfil de Enterprise Management Agent predeterminado.

Perfiles de BlackBerry UEM

Nombre de perfil	Descripción	Tipos de dispositivos compatibles	Clasificado o no clasificado	Para obtener más información
Política				
Knox Service Plugin	Instale y configure Knox Service Plugin.	Android	Clasificado	Gestión de dispositivos con Android con configuraciones de aplicación OEM
Activación	Configure las opciones de activación de los dispositivos para los usuarios (por ejemplo, el tipo de activación y el número y los tipos de dispositivos).	Todos los dispositivos	Clasificado	Creación de perfiles de activación

Nombre de perfil	Descripción	Tipos de dispositivos compatibles	Clasificado o no clasificado	Para obtener más información
BlackBerry Dynamics	Habilite BlackBerry Dynamics para los usuarios y configure las normas de acceso a las aplicaciones, protección de datos y registro.	Todos los dispositivos	Clasificado	Control de BlackBerry Dynamics en dispositivos
Modo de bloqueo de la aplicación	Configure un dispositivo para que ejecute solo las aplicaciones que especifique.	Dispositivos iOS supervisados Dispositivos Samsung Knox activados con MDM Dispositivos Windows 10 Education y Windows 10 Enterprise	Clasificado	Limitación de las aplicaciones que se pueden ejecutar en un dispositivo
Enterprise Management Agent	Configure el modo en que los dispositivos se conectan a UEM para actualizar las aplicaciones o la configuración.	iOS Android Windows	Clasificado	Configuración de cómo los dispositivos se ponen en contacto con BlackBerry UEM para actualizaciones de aplicaciones y configuraciones
iPad compartido	Configure un dispositivo iPad para que puedan compartirlo varios usuarios.	iOS	Clasificado	Creación y gestión de grupos de iPads compartidos
Conformidad				
Conformidad	Defina las condiciones de dispositivo no aceptables en la empresa y configurar las acciones de cumplimiento.	Todos los dispositivos	Clasificado	Cumplimiento de las reglas de los dispositivos
Conformidad (BlackBerry Dynamics)	Este es un perfil de solo lectura que muestra los ajustes de conformidad importados de Good Control a un entorno local de UEM.	Todos los dispositivos	N/A	N/A

Nombre de perfil	Descripción	Tipos de dispositivos compatibles	Clasificado o no clasificado	Para obtener más información
Requisitos de informe especial del dispositivo	Configure las versiones de software que deben instalarse en los dispositivos.	Android	Clasificado	Control del modo en que se instalan las actualizaciones de software en los dispositivos
Correo, calendario y contactos				
Correo	Configure el modo en que los dispositivos se conectan a un servidor de correo del trabajo y sincronizan los mensajes de correo electrónico, las entradas del calendario y los datos del organizador.	Todos los dispositivos	Clasificado	Creación de perfiles de correo electrónico
IMAP/correo electrónico POP3	Configure el modo en que los dispositivos se conectan a un servidor de correo IMAP o POP3 y sincronizan los mensajes de correo electrónico.	Todos los dispositivos	No clasificado	Creación de un perfil de correo IMAP/POP3
Enlace	Especifique los servidores de Microsoft Exchange que se deben utilizar para un enlace automático.	Todos los dispositivos	Clasificado	Creación de un perfil de enlace
CalDAV	Especifique los ajustes del servidor que los dispositivos pueden utilizar para sincronizar la información del calendario.	iOS macOS	No clasificado	Configuración de perfiles CardDAV y CalDAV
CardDAV	Especifique los ajustes del servidor que los dispositivos pueden utilizar para sincronizar la información de los contactos.	iOS macOS	No clasificado	Configuración de perfiles CardDAV y CalDAV
Redes y conexiones				
Wi-Fi	Configure el modo en que los dispositivos se conectan a una red Wi-Fi de trabajo.	Todos los dispositivos	No clasificado	Configuración de las redes Wi-Fi de trabajo para dispositivos

Nombre de perfil	Descripción	Tipos de dispositivos compatibles	Clasificado o no clasificado	Para obtener más información
VPN	Configure el modo en que los dispositivos se conectan a una red VPN de trabajo.	Todos los dispositivos	No clasificado	Configuración de las VPN de trabajo para dispositivos
DNS	Especifique los servidores DNS que utilizan los dispositivos para acceder a dominios específicos.	iOS macOS	Clasificado	Especificación de servidores DNS para dispositivos iOS y macOS
Proxy	Configure el modo en que los dispositivos utilizan un servidor proxy para acceder a los servicios web de Internet o de una red de trabajo.	iOS macOS Android	Clasificado	Configuración de los perfiles de proxy para dispositivos
Conectividad de la empresa	Configure el modo en que los dispositivos pueden conectarse a los recursos de la empresa mediante la conectividad de la empresa y si los dispositivos pueden utilizar BlackBerry Secure Connect Plus.	iOS Android	Clasificado	Uso de BlackBerry Secure Connect Plus en las conexiones con los recursos de trabajo
Conectividad de BlackBerry Dynamics	Configure las conexiones de red, los dominios de Internet, los rangos de direcciones IP y los servidores de aplicaciones a los que los dispositivos se pueden conectar cuando se usan aplicaciones de BlackBerry Dynamics.	Todos los dispositivos	Clasificado	Configuración de conexiones de red para aplicaciones BlackBerry Dynamics
BlackBerry 2FA	Habilite la autenticación de dos factores para los usuarios y configure las funciones de autenticación previa y autorrescate.	iOS Android	Clasificado	Crear un perfil de BlackBerry 2FA
Uso de red	Configure si las aplicaciones de trabajo de los dispositivos iOS pueden utilizar la red móvil o la itinerancia de datos.	iOS	Clasificado	Control del uso de la red de las aplicaciones en los dispositivos iOS
Filtro de contenido web	Limite los sitios web que un usuario puede ver en dispositivos iOS supervisados.	Dispositivos iOS supervisados	No clasificado	Creación de un perfil de filtro de contenido web en dispositivos iOS

Nombre de perfil	Descripción	Tipos de dispositivos compatibles	Clasificado o no clasificado	Para obtener más información
Extensión de registro único	Permita a los dispositivos iOS autenticarse automáticamente con dominios y servicios web en la red de su empresa.	iOS	No clasificado	Habilitación de la autenticación automática para dispositivos iOS
Dominios gestionados	Configure dispositivos iOS para notificar a los usuarios sobre el envío de correos electrónicos fuera de los dominios de confianza y restrinja las aplicaciones que pueden abrir los documentos descargados desde los dominios internos.	iOS	No clasificado	Especificación de dominios de correo electrónico y web para dispositivos iOS
AirPrint	Añada impresoras a las listas de impresoras AirPrint de los usuarios.	iOS	No clasificado	Creación de un perfil AirPrint para dispositivos iOS
AirPlay	Añada dispositivos a las listas de dispositivos AirPlay de los usuarios.	iOS	No clasificado	Creación de un perfil AirPlay para dispositivos iOS
Nombre de punto de acceso	Especifique APN para que los dispositivos los utilicen para conectarse a las operadoras.	Android	No clasificado	Creación de un perfil de nombre de punto de acceso para dispositivos Android
Protección				
Windows Information Protection	Configure el ajuste de Protección de la información de Windows en Windows 10.	Windows 10	Clasificado	Configuración de Windows Information Protection para dispositivos con Windows 10
Protección de aplicaciones de Microsoft Intune	Configure cómo se protegen los datos en las aplicaciones Office 365.	iOS Android	No clasificado	Gestión de aplicaciones protegidas mediante Microsoft Intune
Servicio de ubicación	Solicite la ubicación de los dispositivos y vea la ubicación aproximada de los mismos en un mapa.	iOS Android Windows	Clasificado	Uso de servicios de ubicación en los dispositivos

Nombre de perfil	Descripción	Tipos de dispositivos compatibles	Clasificado o no clasificado	Para obtener más información
No molestar	Bloquee las notificaciones de BlackBerry Work durante los periodos de inactividad.	iOS Android	Clasificado	Desactivación de las notificaciones fuera del horario laboral de BlackBerry Work
Protección contra el restablecimiento de los datos de fábrica	Controlar la función de protección contra el restablecimiento de los datos de fábrica en los dispositivos Android.	Android	Clasificado	Gestión de la protección contra el restablecimiento de los datos de fábrica para dispositivos Android Enterprise y Android Management
CylancePROTECT	Configure las funciones de seguridad de CylancePROTECT Mobile for BlackBerry UEM.	iOS Android	Clasificado	CylancePROTECT Mobile para BlackBerry UEM
Personalizada				
Dispositivo	Especifique la información que se muestra en los dispositivos.	iOS Android Windows	Clasificado	Presentación de la información de la empresa en los dispositivos
Diseño de la pantalla de inicio	Configure el diseño de las aplicaciones en los dispositivos con iOS.	iOS	Clasificado	Configuración del diseño de las aplicaciones en dispositivos iOS
Cargas personalizadas	Especifique la información de configuración personalizada del dispositivo mediante un código de carga.	iOS	No clasificado	Administración de las funciones de iOS mediante perfiles de carga personalizados
Notificación por aplicación	Configure los ajustes de notificación para las aplicaciones del sistema y las aplicaciones que gestiona mediante UEM.	Dispositivos iOS supervisados	Clasificado	Gestión de notificaciones de aplicaciones en dispositivos iOS supervisados
Certificados				

Nombre de perfil	Descripción	Tipos de dispositivos compatibles	Clasificado o no clasificado	Para obtener más información
Certificado de CA	Especifique un certificado de CA que los dispositivos puedan utilizar para establecer una conexión de confianza con una red o servidor de trabajo.	Todos los dispositivos	No clasificado	Envío de certificados de CA a dispositivos y aplicaciones
Certificado compartido	Especifique un certificado de cliente que los dispositivos puedan utilizar para autenticar usuarios en una red o servidor de trabajo.	iOS macOS Android	No clasificado	Envío del mismo certificado de cliente a varios dispositivos
Credencial de usuario	Especifique la conexión de CA que los dispositivos utilizan para obtener un certificado de cliente que se usa para autenticarse en una red o servidor de trabajo.	iOS macOS Android	No clasificado	Envío de certificados de cliente a dispositivos y aplicaciones mediante perfiles de credenciales de usuario
SCEP	Especifique el servidor SCEP que los dispositivos utilizan para obtener un certificado de cliente que se usa para autenticarse en una red o servidor de trabajo.	Todos los dispositivos	No clasificado	Envío de certificados de cliente a dispositivos y aplicaciones mediante SCEP
OCSP	Permita que los dispositivos comprueben el estado de los certificados S/MIME.	iOS Android	Clasificado	Determinación del estado de los certificados S/MIME en dispositivos
CRL	Configure UEM para buscar el estado de los certificados S/MIME.	iOS Android	Clasificado	Determinación del estado de los certificados S/MIME en dispositivos
Perfil de asignación de certificados	Especifique los certificados de cliente que deben utilizar las aplicaciones.	Android	Clasificado	Especificación del certificado que usa una aplicación mediante un perfil de asignación de certificados

Administración de perfiles

1. En la barra de menús de la consola de administración, haga clic en **Políticas y perfiles**.
2. Haga clic en el tipo de perfil adecuado.

3. Efectúe una de las acciones siguientes:

Tarea	Pasos
Copie un perfil.	**a.** Haga clic en el nombre del perfil que desea copiar. **b.** Haga clic en . **c.** Escriba un nombre y una descripción para el perfil. **d.** Configure los valores adecuados para el perfil. Para obtener más información sobre cada tipo de perfil, consulte Perfiles de BlackBerry UEM. **e.** Haga clic en **Guardar**. **f.** Asigne el perfil a usuarios y grupos.
Cambie un perfil.	**a.** Haga clic en el nombre del perfil que desea cambiar. **b.** Haga clic en . **c.** Realice cambios en el perfil. **d.** Haga clic en **Guardar**.
Clasifique los perfiles.	**a.** Haga clic en . **b.** Utilice las flechas para mover los perfiles hacia arriba o hacia abajo en la clasificación. **c.** Haga clic en **Guardar**.
Elimine un perfil de las cuentas de usuario.	**a.** Haga clic en el nombre del perfil que desea eliminar. **b.** En la pestaña **Asignado a x usuarios**, busque y seleccione las cuentas de usuario de las que desea eliminar el perfil. **c.** Haga clic en .
Elimine un perfil de los grupos.	**a.** Haga clic en el nombre del perfil que desea eliminar. **b.** En la pestaña **Asignado a x grupos**, busque y seleccione los grupos de los que desea eliminar el perfil. **c.** Haga clic en .
Elimine un perfil.	No puede eliminar un perfil predeterminado. Cuando se elimina un perfil personalizado, UEM lo elimina de los usuarios y dispositivos a los que está asignado. **a.** Seleccione el perfil que desea eliminar. **b.** Haga clic en . **c.** Haga clic en **Eliminar**.

Uso de variables en perfiles, correos electrónicos y notificaciones

BlackBerry UEM admite variables predeterminadas y personalizadas que puede utilizar en perfiles, notificaciones de cumplimiento, correos electrónicos de activación y notificaciones de eventos para personalizar configuraciones y mensajes para usuarios individuales. Las variables predeterminadas representan atributos de cuenta estándar (por ejemplo, nombre de usuario, correo electrónico) y otros atributos predefinidos (por ejemplo, dirección del servidor utilizada para la activación del dispositivo). Puede utilizar las variables personalizadas para definir atributos adicionales.

Puede utilizar una variable en cualquier campo de texto de un perfil, salvo en los campos Nombre y Descripción. Por ejemplo, puede especificar "%UserName%@example.com" en el campo Dirección de correo de un perfil de correo.

Puede ver la lista de variables predeterminadas que están disponibles para su uso en la consola de administración en **Configuración > Configuración general > Variables predeterminadas.**

Tenga en cuenta que las políticas de TI y las configuraciones de aplicaciones de BlackBerry Dynamics no son compatibles con el uso de variables.

Definición de variables personalizadas

Puede definir hasta cinco variables de texto personalizadas y hasta cinco variables de texto enmascarado para representar información confidencial, como contraseñas. Cuando se define una variable personalizada, se especifica una etiqueta para la variable (por ejemplo, contraseña de VPN). Al crear o actualizar una cuenta de usuario, las etiquetas se utilizan como nombres de campo en la sección Variables personalizadas y se pueden especificar los valores apropiados para ese usuario. Todas las cuentas de usuario admiten variables personalizadas, incluidas las cuentas de administrador. Puede utilizar las variables personalizadas de la misma forma que utiliza las variables predeterminadas.

1. En la barra de menús de la consola de administración, haga clic en **Configuración > Configuración general > Valores personalizados**.
2. Seleccione la casilla de verificación **Mostrar variables personalizadas al agregar o editar un usuario**.
3. Especifique una etiqueta para cada variable personalizada que tenga pensado utilizar.
4. Haga clic en **Guardar**.

Uso de plantillas de correo electrónico para enviar mensajes a los usuarios

Puede utilizar plantillas de correo electrónico para adaptar y personalizar los mensajes de correo electrónico que BlackBerry UEM envía a los usuarios por diversos motivos, como proporcionar instrucciones para la activación del dispositivo, notificar a los usuarios sobre problemas de conformidad y proporcionar claves de acceso para las aplicaciones de BlackBerry Dynamics.

Puede personalizar los mensajes de correo electrónico utilizando variables para elementos como el nombre, la dirección de correo electrónico o la contraseña de activación del usuario, y puede personalizar el aspecto de los mensajes utilizando diferentes tipos de letra, colores e imágenes. Puede crear varias plantillas que se utilizarán para distintos tipos de dispositivos o tipos de activación. Puede editar las plantillas de correo electrónico predeterminadas o bien crear otras nuevas.

Al realizar diversas tareas en la consola de administración (por ejemplo, añadir un usuario, crear un perfil de conformidad, etc.), puede seleccionar la plantilla de correo electrónico que desea que UEM utilice para enviar un mensaje a los usuarios del dispositivo.

Puede ver las plantillas predeterminadas disponibles en la consola de administración en **Configuración > Configuración general > Plantillas**.

Edición de una plantilla de correo

Si decide cambiar una plantilla de correo electrónico predeterminada, se recomienda que guarde una copia de seguridad del texto de la plantilla original por si desea restaurarla más adelante.

1. En la barra de menús de la consola de administración, haga clic en **Configuración > Configuración general > Plantillas**.
2. Haga clic en la plantilla que desea editar.
3. Edite los campos **Nombre**, **Asunto** o **Mensaje** según sea necesario.
4. Haga clic en **Guardar**.

Creación de una plantilla de correo de activación

1. En la barra de menús de la consola de administración, haga clic en **Configuración > Configuración general > Plantillas**.
2. Haga clic en + > **Activación de dispositivos**.
3. En el campo **Nombre**, escriba un nombre para la plantilla.
4. En el campo **Asunto**, escriba el asunto del correo electrónico de activación.
5. En el campo **Mensaje**, escriba el texto del cuerpo del correo electrónico de activación.

   Utilice el editor HTML para personalizar el formato, insertar imágenes (por ejemplo, un logotipo corporativo), etc. Puede insertar variables para personalizar partes del correo electrónico. Consulte Uso de variables en perfiles, correos electrónicos y notificaciones.
6. Si desea que los usuarios activen sus dispositivos mediante QR Code en lugar de una contraseña de activación, active la casilla de verificación **Adjuntar un código QR al mensaje de correo para la activación de dispositivos iOS y Android**.
7. Para enviar la contraseña de activación o QR Code por separado de las instrucciones de activación, seleccione **Enviar dos correos electrónicos de activación individuales: uno para las instrucciones completas y otro**

para la contraseña y especifique el contenido y las opciones del segundo correo electrónico de activación. Si decide enviar solo un correo de activación, asegúrese de incluir la contraseña de activación, la variable de la contraseña de activación o el QR Code en el primer correo.

8. Haga clic en **Guardar**.

Para obtener más información sobre la activación de dispositivos, consulte Activación de dispositivos.

Creación de una plantilla para las notificaciones de conformidad

Cuando el dispositivo de un usuario no cumple los requisitos que ha configurado en un perfil de conformidad asignado, BlackBerry UEM puede enviar un mensaje de correo electrónico personalizado al usuario en función de una plantilla especificada. UEM Incluye una plantilla de correo electrónico predeterminada de infracción de conformidad que se puede editar, pero no borrar. Si no asigna una plantilla diferente a una cuenta de usuario, UEM utiliza la plantilla predeterminada.

1. En la barra de menús de la consola de administración, haga clic en **Configuración > Configuración general > Plantillas**.
2. Haga clic en + > **Infracción de conformidad**.
3. En el campo **Nombre**, escriba un nombre para la plantilla.
4. En el campo **Asunto**, escriba un asunto para el mensaje.
5. En el campo **Mensaje**, el texto del cuerpo del mensaje de correo electrónico de conformidad.

   Utilice el editor HTML para personalizar el formato, insertar imágenes (por ejemplo, un logotipo corporativo), etc. Puede insertar variables para personalizar partes del correo electrónico. Consulte Uso de variables en perfiles, correos electrónicos y notificaciones.
6. Haga clic en **Guardar**.

Para obtener más información acerca de la conformidad del dispositivo, consulte Cumplimiento de las reglas de los dispositivos.

Crear una plantilla de correo de notificación de evento

Puede crear una plantilla de correo electrónico de notificación de eventos que BlackBerry UEM pueda utilizar para enviar mensajes personalizados a los administradores cuando se produzcan determinados eventos en el entorno UEM de su empresa.

1. En la barra de menús de la consola de administración, haga clic en **Configuración > Configuración general > Plantillas**.
2. Haga clic en + > **Notificaciones de eventos**.
3. En el campo **Nombre**, escriba un nombre para la plantilla.
4. En el campo **Asunto**, escriba un asunto para el mensaje de correo electrónico. Si desea adjuntar el tipo de evento a la línea de asunto, seleccione la casilla de verificación **Adjuntar tipo de evento al asunto del correo**.
5. En el campo **Mensaje**, escriba el texto del cuerpo del correo electrónico de notificación de evento.

   Utilice el editor HTML para personalizar el formato, insertar imágenes (por ejemplo, un logotipo corporativo), etc. Puede insertar variables para personalizar partes del correo electrónico. Consulte Uso de variables en perfiles, correos electrónicos y notificaciones.
6. Haga clic en **Guardar**.

Para obtener más información sobre notificaciones de eventos, consulte Creación de notificaciones de eventos.

Plantilla de texto sugerido

El texto sugerido a continuación se utiliza en las plantillas de correo electrónico predeterminadas. Si edita las plantillas de correo predeterminadas y más adelante desea utilizar el texto predeterminado, puede copiarlo y pegarlo desde aquí.

Nombre	Texto sugerido
Código de activación del perfil de trabajo de Android	**Asunto: Se ha creado su código de activación del perfil de trabajo de Android** %UserDisplayName%, Para activar un dispositivo con Android con solo perfil de trabajo, el administrador ha creado su código de activación del perfil de trabajo Android. Recibirá su contraseña de activación de BlackBerry UEM en otro mensaje de correo. Su código de activación del perfil de trabajo de Android:%GoogleActivationCode% Su código de activación del perfil de trabajo de Android caducará el %ActivationPasswordExpiry%. Si tiene alguna pregunta, póngase en contacto con el administrador.
Credenciales predeterminadas de cuenta de Google gestionada	**Asunto: Se le ha creado una cuenta de Google** %UserDisplayName%, Para activar el perfil de trabajo en el dispositivo, el administrador le ha creado una cuenta de Google. Necesitará la contraseña de su cuenta de Google cuando active el perfil de trabajo. La contraseña de la cuenta de Google que se muestra aquí no es la contraseña que debe utilizar al activar su dispositivo en BlackBerry UEM. Recibirá su contraseña de activación de BlackBerry UEM en otro mensaje de correo, o bien pueden configurar su contraseña de activación de BlackBerry UEM en BlackBerry UEM Self-Service. Necesitará la siguiente información cuando active el perfil de trabajo: • La dirección de correo de trabajo: %UserEmailAddress% • La contraseña de la cuenta Google: %Password% Puede gestionar su cuenta de Google en https://myaccount.google.com. Si cambia la contraseña de su cuenta de Google, la contraseña incluida en este correo ya no podrá aplicarse y deberá utilizar la nueva contraseña. Conserve esta información para su referencia en el futuro. Si tiene alguna pregunta, póngase en contacto con el administrador.

Nombre	Texto sugerido
Correo de activación de dispositivos en DEP de Apple Primero correo	**Asunto: Activación de su dispositivo en BlackBerry UEM** %UserDisplayName%, El administrador ha activado el dispositivo con iOS de BlackBerry UEM. Para activar el dispositivo, necesita la siguiente información: • La dirección de correo de trabajo: %UserEmailAddress% • La contraseña de activación del dispositivo: la contraseña de activación se enviará en un mensaje de correo independiente. Puede gestionar su propio dispositivo con BlackBerry UEM Self-Service en %UserSelfServicePortalURL%. Para iniciar sesión, utilice el siguiente nombre de usuario: Nombre de usuario de BlackBerry UEM Self-Service: %UserName% Puede que haya recibido la contraseña de BlackBerry UEM Self-Service en otro correo. Si no la ha recibido, póngase en contacto con el administrador. Conserve esta información para su referencia en el futuro. Si tiene alguna pregunta, póngase en contacto con el administrador.
Correo de activación de dispositivos en DEP de Apple Segundo mensaje de correo	**Asunto: Contraseña para activar su dispositivo en BlackBerry UEM** %UserDisplayName%, El administrador ha activado su dispositivo móvil para BlackBerry UEM. Para activar el dispositivo, necesita la siguiente información: Contraseña de activación del dispositivo: %ActivationPassword% La contraseña caducará el %ActivationPasswordExpiry%. Siga las instrucciones del correo "Activación de su dispositivo en BlackBerry UEM" para activar el dispositivo iOS en BlackBerry UEM. Si tiene alguna pregunta, póngase en contacto con el administrador. ¡Bienvenido a BlackBerry UEM !

Nombre	Texto sugerido
Correo de clave de acceso de BlackBerry Dynamics	**Asunto: Se ha creado una clave de acceso para una aplicación de BlackBerry Dynamics para usted** %UserDisplayName%, El administrador ha creado una clave de acceso para una aplicación de BlackBerry Dynamics. Este correo contiene la clave de acceso y las instrucciones para configurar la aplicación. Si dispone de permiso para utilizar más de una aplicación, recibirá más de un correo. Cada correo incluye una clave de acceso que se puede utilizar para configurar una aplicación. Puede utilizar cualquiera de las claves de acceso para configurar cualquiera de las aplicaciones, pero solo puede utilizar cada clave una única vez. Antes de comenzar, asegúrese de que dispone de datos móviles o cobertura Wi-Fi. **1.** Abra la aplicación BlackBerry Dynamics. **2.** Cuando se le solicite, proporcione la siguiente información. • Dirección de correo: %UserEmailAddress% • Clave de acceso: %AccessKeys% La clave de acceso caducará el %AccessKeyExpiry%. **3.** Puede que se le pida que cree una contraseña. Deberá introducir esta contraseña cuando abra la aplicación. Si tiene alguna pregunta, póngase en contacto con el administrador.

Nombre	Texto sugerido
Correo electrónico de activación predeterminado Primero correo	**Asunto: Activación de su dispositivo en BlackBerry UEM** %UserDisplayName%, El administrador ha activado su dispositivo móvil para BlackBerry UEM. Para activar el dispositivo, se requiere toda o parte de la siguiente información: • La dirección de correo de trabajo: %UserEmailAddress% • Nombre del servidor: %ActivationURL% • Nombre de usuario de activación: %ActivationUserName% • La contraseña de activación del dispositivo: la contraseña de activación se enviará en un mensaje de correo independiente. Para los dispositivos Android: Si utiliza un dispositivo Android, debe instalar BlackBerry UEM Client desde Google Play. Para los dispositivos iOS: Si utiliza un dispositivo iOS, debe instalar BlackBerry UEM Client desde la App Store. Para los dispositivos iOS, abra Safari y vaya a workspace://apps para instalar las aplicaciones que su administrador le haya asignado. Si está disponible, también puede tocar la opción Work Apps en el dispositivo. Para los dispositivos macOS: Si utiliza un dispositivo macOS, debe activar el dispositivo mediante BlackBerry UEM Self-Service. Para dispositivos con Windows 10 o versiones posteriores: Necesitará la siguiente información para activar el dispositivo: • Nombre del servidor: %ClientlessActivationURL% • URL del servidor de certificados: %RsaRootCaCertUrl% • Debe instalar el certificado RSA. Escriba la URL del servidor de certificados en la barra de direcciones del navegador del dispositivo. Siga las instrucciones e instale el certificado en la carpeta Autoridades de certificación raíz de confianza. • En el dispositivo, vaya a **Configuración > Cuentas > Acceso al trabajo o la escuela** y toque Inscribirse solo en la administración de dispositivos. Para gestionar los dispositivos Puede gestionar su propio dispositivo con BlackBerry UEM Self-Service en %UserSelfServicePortalURL%. Para iniciar sesión, utilice el siguiente nombre de usuario: Nombre de usuario de BlackBerry UEM Self-Service: %UserName% Puede que haya recibido la contraseña de BlackBerry UEM Self-Service en otro correo. ¡Bienvenido a BlackBerry UEM !

Nombre	Texto sugerido
Correo electrónico de activación predeterminado Segundo mensaje de correo	**Asunto: Contraseña para activar su dispositivo en BlackBerry UEM** %UserDisplayName%, El administrador ha activado su dispositivo móvil para BlackBerry UEM. Para activar el dispositivo, necesita la siguiente información: • Contraseña de activación del dispositivo: %ActivationPassword% • La contraseña caducará el %ActivationPasswordExpiry% Siga las instrucciones del correo "Activación de su dispositivo en BlackBerry UEM" para activar el dispositivo con iOS, Android o Windows en BlackBerry UEM. Si tiene alguna pregunta, póngase en contacto con el administrador. ¡Bienvenido a BlackBerry UEM !
Correo electrónico de activación de Android Management predeterminado	**Asunto: Activación de su dispositivo en BlackBerry UEM** %UserDisplayName%, Su administrador ha activado Android Management en su dispositivo para que se pueda crear un perfil de trabajo. Para crear el perfil de trabajo, puede hacer clic en el siguiente enlace %ActivationAndroidManagementURL% desde el dispositivo. También puede escanear el código QR en su dispositivo. Vaya a **Configuración > Servicios de Google > Configurar y restaurar > Configurar su perfil de trabajo y**, a continuación, escanee el siguiente código QR. El enlace de activación y el código QR caducarán el %ActivationPasswordExpiry%. %ActivationAndroidManagementQRCode% Conserve esta información para su referencia en el futuro. Si tiene alguna pregunta, póngase en contacto con el administrador.
Correo de conformidad predeterminado	**Asunto: Notificación de dispositivo no conforme** Su dispositivo no cumple las políticas de su empresa. De mantener esta condición, el administrador podría limitar el acceso a los datos de la empresa desde el dispositivo, eliminar los datos de la empresa en el dispositivo o eliminar todo el contenido y la configuración del dispositivo.

Nombre	Texto sugerido
Correo electrónico de activación predeterminado de Solo espacio de trabajo (Android Enterprise) Primero correo	**Asunto: Activación de su dispositivo en BlackBerry UEM** %UserDisplayName%, El administrador ha activado su dispositivo con Android (9.0 y posterior) para BlackBerry UEM. Para activar el dispositivo, necesita la siguiente información: • Nombre de usuario de activación: %ActivationUserName% • La contraseña de activación del dispositivo: la contraseña de activación se enviará en un mensaje de correo independiente. Para activar el dispositivo, realice las acciones siguientes: **1.** Si no ve la pantalla de bienvenida de configuración del dispositivo, restablezca el dispositivo con la configuración predeterminada de fábrica. **2.** Durante la configuración del dispositivo, en la pantalla Agregar su cuenta, introduzca las credenciales de su cuenta de Google. Espere mientras el dispositivo actualiza algunas aplicaciones importantes del sistema y descarga UEM Client. **3.** En BlackBerry UEM Client, siga las instrucciones que aparecen en la pantalla para activar el dispositivo. Puede gestionar su propio dispositivo con BlackBerry UEM Self-Service en %UserSelfServicePortalURL%. Para iniciar sesión, utilice el siguiente nombre de usuario: Nombre de usuario de BlackBerry UEM Self-Service: %UserName% Puede que haya recibido la contraseña de BlackBerry UEM Self-Service en otro correo. Si no la ha recibido, póngase en contacto con el administrador. Conserve esta información para su referencia en el futuro. Si tiene alguna pregunta, póngase en contacto con el administrador. ¡Bienvenido a BlackBerry UEM !
Correo de activación de Solo espacio de trabajo (perfiles de trabajo de Android) predeterminada Segundo mensaje de correo	**Asunto: Contraseña para activar su dispositivo en BlackBerry UEM** %UserDisplayName%, El administrador ha activado el dispositivo con Android para BlackBerry UEM. Para activar el dispositivo, necesita la siguiente información: • Contraseña de activación del dispositivo: %ActivationPassword% • La contraseña caducará el %ActivationPasswordExpiry% Siga las instrucciones del correo "Activación de su dispositivo en BlackBerry UEM" para activar el dispositivo en BlackBerry UEM. Si tiene alguna pregunta, póngase en contacto con el administrador. Le damos la bienvenida a BlackBerry UEM
Correo de notificación de eventos de BlackBerry UEM	**Asunto: Notificación de eventos de BlackBerry UEM** Se ha producido el siguiente evento: %AllEventVariables%

Nombre	Texto sugerido
Notificación de dispositivo activado	**Asunto: Dispositivo activado en BlackBerry UEM** %UserDisplayName%, Se ha activado el dispositivo en BlackBerry UEM. Información del dispositivo Modelo: %DeviceModel% Número de serie: %SerialNumber% IMEI: %DeviceIMEI% Si no ha activado este dispositivo, póngase en contacto con el administrador. **Asunto: Dispositivo BlackBerry Dynamics activado en BlackBerry UEM** %UserDisplayName%, Se ha activado el dispositivo BlackBerry Dynamics en BlackBerry UEM. Si no ha activado este dispositivo, póngase en contacto con el administrador.
Notificación de inicio de sesión de autoservicio	**Asunto: Notificación de inicio de sesión de autoservicio** %UserDisplayName%, Ha iniciado sesión en BlackBerry UEM Self-Service. Dirección IP: %IPAddress% Hora: %Timestamp% Si no ha iniciado sesión, póngase en contacto con el administrador.

Gestión de dispositivos con políticas de TI

Puede utilizar las políticas de TI para gestionar la seguridad y el comportamiento de los dispositivos en el entorno BlackBerry UEM de la empresa. Una política de TI es un conjunto de reglas que puede utilizar para controlar las características y la funcionalidad del dispositivo. Por ejemplo, puede utilizar reglas de política de TI para imponer requisitos de contraseña, impedir el uso de determinadas características del dispositivo (por ejemplo, la cámara) y controlar la disponibilidad de ciertas aplicaciones.

Puede configurar las reglas de todos los tipos de dispositivos en la misma política de TI. El sistema operativo del dispositivo determina las características que pueden controlarse mediante las reglas de la política de TI. El tipo de activación del dispositivo determina qué reglas se aplican a un dispositivo específico y si puede utilizar reglas para controlar todo el dispositivo o solo el espacio de trabajo. Los dispositivos ignoran las reglas de políticas de TI que no son aplicables.

Descargue la hoja de cálculo de reglas de políticas de TI para obtener una referencia completa de todas las reglas de políticas de TI disponibles para cada tipo de dispositivo UEM compatible.

UEM incluye una política de TI predeterminada con reglas preconfiguradas para cada tipo de dispositivo. Puede cambiar la política de TI predeterminada para satisfacer las necesidades de su empresa. Si no se asigna ninguna política de TI a una cuenta de usuario, a un grupo de usuarios al que pertenece el usuario o a un grupo de dispositivos a los que pertenecen los dispositivos del usuario, UEM envía la política de TI predeterminada a los dispositivos del usuario. UEM envía automáticamente una política de TI a un dispositivo cuando el usuario lo activa, cuando se actualiza una política de TI asignada o cuando una política de TI diferente está asignada a una cuenta de usuario o de dispositivo.

UEM asigna solo una política de TI a un dispositivo y utiliza reglas predefinidas para determinar la política de TI que se asigna. Una política de TI asignada directamente a un usuario tiene prioridad sobre una política de TI asignada a través de la pertenencia a un grupo de usuarios. Si un usuario es miembro de varios grupos de usuarios con diferentes políticas de TI, se utiliza la clasificación para determinar la política de TI que se asigna. Si el dispositivo de un usuario pertenece a un grupo de dispositivos, la política de TI asignada al grupo de dispositivos tiene prioridad sobre una política de TI que se asigne directamente al usuario. Si el dispositivo pertenece a varios grupos de dispositivos con diferentes políticas de TI, se utiliza la clasificación para determinar la política de TI que se asigna.

Administración de políticas de TI

Puede cambiar la política de TI predeterminada o puede crear y asignar políticas de TI personalizadas.

1. En la barra de menús de la consola de administración, haga clic en **Políticas y perfiles > Política > Políticas de TI**.
2. Efectúe una de las acciones siguientes:

Tarea	Pasos
Cree una política de TI.	**a.** Haga clic en +. **b.** Escriba un nombre y una descripción para la política de TI. **c.** Haga clic en la pestaña de cada tipo de dispositivo y configure los valores adecuados para las reglas de la política de TI. Para obtener más información acerca de las reglas de políticas de TI, consulte la hoja de cálculo de las reglas de políticas de TI. **d.** Haga clic en **Guardar**. **e.** Asigne la política de autenticación a los usuarios o grupos.

Tarea	Pasos
Copie una política de TI.	**a.** Haga clic en el nombre de la política de TI que desea copiar. **b.** Haga clic en . **c.** Escriba un nombre y una descripción para la política de TI. **d.** Haga clic en la pestaña de cada tipo de dispositivo y configure los valores adecuados para las reglas de la política de TI. Para obtener más información acerca de las reglas de políticas de TI, consulte la hoja de cálculo de las reglas de políticas de TI. **e.** Haga clic en **Guardar**. **f.** Asigne la política de autenticación a los usuarios o grupos.
Cambie una política de TI.	**a.** Haga clic en el nombre de la política de TI que desee cambiar. **b.** Haga clic en . **c.** Realice modificaciones en la pestaña adecuada para cada tipo de dispositivo. **d.** Haga clic en **Guardar**.
Clasifique las políticas de TI.	**a.** Haga clic en . **b.** Utilice las flechas para mover las políticas de TI hacia arriba o hacia abajo en la clasificación. **c.** Haga clic en **Guardar**.
Elimine una política de TI de las cuentas de usuario.	**a.** Haga clic en el nombre de la política de TI que desea eliminar. **b.** En la pestaña **Asignado a x usuarios**, busque las cuentas de usuario de las que desea eliminar la política de TI y selecciónelas. **c.** Haga clic en .
Elimine una política de TI de los grupos.	**a.** Haga clic en el nombre de la política de TI que desea eliminar. **b.** En la pestaña **Asignado a x grupos**, busque los grupos de los que desea eliminar la política de TI y selecciónelos. **c.** Haga clic en .
Elimine una política de TI.	No puede eliminar la política de TI predeterminada. Cuando se elimina una política de TI personalizada, UEM elimina la política de TI de los usuarios y dispositivos a los que está asignada. **a.** Seleccione la política de TI que desea eliminar. **b.** Haga clic en . **c.** Haga clic en **Eliminar**.
Exporte políticas de TI a un archivo .xml.	**a.** Seleccione las políticas de TI que desea exportar. **b.** Haga clic en .

Importación de las políticas de TI y las actualizaciones de metadatos del dispositivo manualmente

BlackBerry envía regularmente actualizaciones de las políticas de TI y de los metadatos de los dispositivos a BlackBerry UEM. Por ejemplo, cuando un proveedor lanza un nuevo modelo de dispositivo, BlackBerry puede enviar metadatos actualizados del dispositivo a UEM para que los perfiles de activación y conformidad incluyan el nuevo modelo de dispositivo. Cuando un proveedor publica una actualización del sistema operativo, se puede enviar un nuevo paquete de políticas de TI a UEM para que pueda administrar nuevas funciones del sistema operativo.

De forma predeterminada, UEM recibe e instala estas actualizaciones automáticamente. Si la política de seguridad de su empresa no permite las actualizaciones automáticas y tiene un entorno local de UEM, puede desactivarlas e importar actualizaciones de forma manual. Los archivos de actualización se acumulan. Si se pierde una actualización, la siguiente instalará todas las reglas de políticas de TI o los metadatos de dispositivos que se actualizaron anteriormente. Puede configurar notificaciones de eventos para informar a los administradores cuando se instalen actualizaciones de las políticas de TI y de los metadatos de los dispositivos.

Antes de empezar: Descargue el conjunto de metadatos o de políticas de TI siguiendo las instrucciones incluidas en el correo electrónico de notificación de actualización de BlackBerry.

1. En la barra de menús de la consola de administración, haga clic en **Configuración > Infraestructura > Importar datos de configuración**.
2. Efectúe una de las acciones siguientes:
   - Para desactivar las actualizaciones automáticas de los conjuntos de políticas de TI, desmarque la casilla de verificación **Actualizar automáticamente datos de conjuntos de políticas de TI**.
   - Para desactivar las actualizaciones automáticas de los metadatos de dispositivos, desmarque la casilla de verificación **Actualizar automáticamente metadatos de dispositivos**.
3. Haga clic en el botón **Examinar** adecuado para ir al archivo de datos que desea importar y selecciónelo. Haga clic en **Abrir**.

Creación de mensajes de compatibilidad de dispositivos para las funciones desactivadas en los dispositivos Android

En los dispositivos Android, puede crear un mensaje de ayuda que se muestra en el dispositivo cuando una función se desactiva debido a una política de TI. El mensaje se muestra en la pantalla de configuración para la función que está desactivada. Si no crea un mensaje de ayuda, el dispositivo muestra el mensaje predeterminado del sistema operativo.

1. En la barra de menús de la consola de administración, haga clic en **Configuración > Configuración general > Mensajes personalizados de ayuda del dispositivo**.
2. En la lista desplegable **Idioma del dispositivo**, seleccione el idioma en el que desea que se muestre la notificación.
3. En el campo **Aviso de funciones desactivadas**, escriba el aviso que desea que se muestre en los dispositivos cuando una función está desactivada.
4. Opcionalmente, en el campo **Mensaje de ayuda de administrador**, escriba un aviso para que se muestre en la pantalla de configuración Administradores del dispositivo.
5. Si desea crear un mensaje en más de un idioma, haga clic en **Agregar un idioma adicional** y repita los pasos previos.
6. Si ha añadido mensajes en más de un idioma, seleccione el botón de opción **Idioma predeterminado** para el idioma que desee utilizar en los dispositivos que no utilicen uno de los idiomas especificados.
7. Haga clic en **Guardar**.

Cumplimiento de las reglas de los dispositivos

Puede utilizar los perfiles de conformidad para alentar a los usuarios a seguir los estándares de la empresa en el uso de los dispositivos. Un perfil de cumplimiento define las condiciones del dispositivo que no son aceptables en la empresa. Por ejemplo, puede optar por no permitir los dispositivos que se han liberado o tienen acceso a la raíz, o bien aquellos que tienen una alerta de integridad debido al acceso no autorizado al sistema operativo.

Un perfil de conformidad especifica las condiciones que harían que un dispositivo no fuera conforme, las notificaciones que recibe un usuario cuando un dispositivo no es conforme y las medidas que tomará BlackBerry UEM si no se resuelve un problema de conformidad (por ejemplo, limitar el acceso de un usuario a los recursos de la organización, eliminar los datos de trabajo del dispositivo o eliminar todos los datos del dispositivo).

UEM incluye un perfil de conformidad predeterminado. El perfil de conformidad predeterminado no aplica ninguna condición de conformidad. Para aplicar las reglas de conformidad, puede cambiar la configuración del perfil de conformidad predeterminado o puede crear y asignar perfiles de conformidad personalizados. A las cuentas de usuario que no tengan asignado un perfil de conformidad personalizado se les asignará el perfil de conformidad predeterminado.

En el caso de los dispositivos Samsung Knox, puede añadir una lista de aplicaciones restringidas a un perfil de conformidad, pero UEM no aplica las normas de conformidad. En su lugar, la lista de aplicaciones restringidas se envía a los dispositivos y este es el que aplica el cumplimiento. No se podrán instalar aplicaciones restringidas o si ya están instaladas, se desactivarán. Al eliminar una aplicación de la lista de aplicaciones restringidas, la aplicación se vuelve a activar si ya está instalada.

Los perfiles de conformidad de BlackBerry Dynamics se importan desde Good Control cuando sincroniza Good Control con UEM. No puede editar los perfiles de conformidad de BlackBerry Dynamics, pero se pueden utilizar como referencia al crear nuevos perfiles de conformidad en UEM. Los usuarios que se asignaron a un perfil de conformidad en Good Control permanecen asignados al mismo perfil después de que se sincronicen con UEM. Cuando un usuario se asigna a un perfil de conformidad de BlackBerry Dynamics, el perfil de conformidad de BlackBerry Dynamics tiene prioridad sobre las reglas de BlackBerry Dynamics en los perfiles de conformidad de UEM que pudieran asignarse a un usuario.

Creación de un perfil de conformidad

Antes de empezar:

- Si desea definir reglas para restringir o permitir aplicaciones específicas, añada estas aplicaciones a la lista de aplicaciones restringidas. Para obtener más información, consulte Adición de una aplicación a la lista de aplicaciones restringidas. Este paso no se aplica a las aplicaciones integradas para dispositivos iOS supervisados. Para restringir las aplicaciones integradas, debe crear un perfil de conformidad y agregar las aplicaciones a la lista de aplicaciones restringidas del perfil. Para obtener más información, consulte iOS y iPadOS: configuración del perfil de conformidad.
- Si desea enviar una notificación de correo electrónico a los usuarios cuando sus dispositivos no cumplan con los requisitos, edite el correo electrónico de conformidad predeterminado o cree una nueva plantilla de correo electrónico de conformidad.

Nota: Si define reglas para sistemas con jailbreak o rooting, versiones de sistemas operativos restringidas o modelos de dispositivos restringidos, los usuarios no podrán realizar nuevas activaciones para los dispositivos que no cumplan con los requisitos con independencia de la acción de cumplimiento que establezca.

1. En la barra de menús de la consola de administración, haga clic en **Políticas y perfiles > Conformidad > Conformidad**.
2. Haga clic en +.
3. Escriba un nombre y una descripción para el perfil.

4. En la lista desplegable **Mensaje de correo electrónico enviado cuando se detecta una violación de conformidad**, seleccione una plantilla de correo electrónico.

   Este es el correo electrónico de conformidad predeterminado que UEM enviará a un usuario cuando se detecta una infracción de la conformidad. Cuando activa las reglas de cumplimiento en el paso 7, tiene la opción de seleccionar diferentes plantillas de correo electrónico para cada regla de conformidad, cuando corresponda.
5. En la lista desplegable **Intervalo de aplicación**, seleccione la frecuencia de las comprobaciones de conformidad de las aplicaciones BlackBerry Dynamics. No puede configurar el intervalo de aplicación para las comprobaciones de conformidad que no son de BlackBerry Dynamics, ya que se producen a intervalos regulares.
6. Expanda **Notificación de dispositivo enviada cuando se detecta una violación de conformidad** y edite el mensaje según sea necesario. Puede utilizar variables en el mensaje para añadir información específica del usuario, del dispositivo y de conformidad. Consulte Uso de variables en perfiles, correos electrónicos y notificaciones.
7. Haga clic en la pestaña de cada tipo de dispositivo de la empresa y configure los valores apropiados para cada configuración de perfil. Para obtener más información acerca de la configuración de cada perfil, consulte lo siguiente:
   - Común: configuración del perfil de conformidad
   - iOS y iPadOS: configuración del perfil de conformidad
   - macOS: configuración del perfil de conformidad
   - Android: configuración del perfil de conformidad
   - Windows: configuración del perfil de conformidad
8. Haga clic en **Guardar**.

Después de terminar:

- Asigne el perfil a usuarios y grupos.
- Si es necesario, clasifique el perfil.
- Para supervisar los eventos de conformidad detectados por UEM, consulte Supervisión de los eventos de conformidad.

Común: configuración del perfil de conformidad

Para cada regla de conformidad que seleccione en las pestañas del dispositivo, elija la acción que desea que BlackBerry UEM realice si un dispositivo del usuario no cumple los requisitos.

Configuración del perfil de conformidad	Descripción
Comportamiento de aviso	En la configuración se especifica cómo UEM pide al usuario que corrija un problema de conformidad y concede tiempo al usuario para que solucione el problema antes de que actúe o si UEM interviene inmediatamente.

Configuración del perfil de conformidad	Descripción
Método de aviso	Esta configuración especifica si UEM solicita al usuario que corrija un problema de conformidad enviando una notificación al dispositivo o un mensaje de correo electrónico y una notificación al dispositivo. Las aplicaciones de BlackBerry Dynamics solo proporcionan notificaciones del dispositivo, independientemente de esta configuración. Los dispositivos con Windows 10 no son compatibles con las notificaciones de dispositivos. Esta configuración solo es válida si "Comportamiento de aviso" está establecida en "Aviso sobre conformidad".
Plantilla de correo electrónico utilizada cuando se detecta una infracción de conformidad	Esta configuración especifica la plantilla de correo electrónico que se debe enviar a un usuario cuando el dispositivo del usuario no cumple la regla de conformidad seleccionada. Si selecciona "Usar perfil predeterminado", UEM envía la plantilla de correo electrónico predeterminada que configuró para el perfil (correo electrónico enviado cuando se detecta una infracción). Esta configuración solo es válida si "Método de aviso" se establece en "Notificaciones de correo electrónico y del dispositivo".
Recuento de avisos	En la configuración se especifica el número de veces que se solicita al usuario que corrija un problema de conformidad. Esta configuración solo es válida si "Comportamiento de aviso" está establecida en "Aviso sobre conformidad".
Intervalo de aviso	En la configuración se especifica el tiempo entre avisos, en minutos, horas o días. Esta configuración solo es válida si "Comportamiento de aviso" está establecida en "Aviso sobre conformidad".

Configuración del perfil de conformidad	Descripción
Acción de cumplimiento para dispositivo	Esta configuración especifica la acción que UEM realiza en dispositivos que no cumplen los requisitos. Las opciones disponibles pueden variar en función del SO y del tipo de regla de conformidad: • Supervisar y registrar: UEM identifica la infracción de conformidad pero no realiza ninguna acción de cumplimiento en el dispositivo. • No confiar: el usuario no puede acceder a los recursos de trabajo ni a las aplicaciones del dispositivo. Los datos y las aplicaciones no se eliminan. En dispositivos con iOS y iPadOS, la cuenta de correo electrónico de trabajo se elimina de la aplicación de correo electrónico nativa. Los usuarios deben restaurar la configuración de la cuenta de correo en la aplicación después de que el dispositivo vuelva a cumplir los requisitos. • Eliminar solo los datos de trabajo • Eliminar todos los datos • Eliminar del servidor Esta configuración no se aplica a dispositivos activados con Privacidad del usuario. En los dispositivos activados con "Trabajo y personal: privacidad de usuario", no se pueden eliminar todos los datos del dispositivo del usuario. Si selecciona "Eliminar todos los datos", UEM realiza la misma acción que "Eliminar solo los datos de trabajo". Para dispositivos supervisados con iOS y iPadOS, las acciones de cumplimiento para la regla "La aplicación restringida está instalada" no son aplicables. Se impide automáticamente que los usuarios instalen aplicaciones restringidas.
Acción de cumplimiento para las aplicaciones de BlackBerry Dynamics	Esta configuración especifica lo que ocurre con las aplicaciones de BlackBerry Dynamics cuando un dispositivo no está en conformidad: • No permitir la ejecución de aplicaciones de BlackBerry Dynamics • Eliminar datos de aplicaciones BlackBerry Dynamics • Supervisar y registrar: UEM identifica la infracción de conformidad, pero no realiza ninguna acción de cumplimiento.

iOS y iPadOS: configuración del perfil de conformidad

Consulte Común: configuración del perfil de conformidad para obtener una explicación sobre las acciones de cumplimiento que BlackBerry UEM puede llevar a cabo si un dispositivo infringe una regla de conformidad.

Configuración del perfil de conformidad	Descripción
SO liberado	Esta configuración crea una regla de conformidad para garantizar que los dispositivos no se liberen. Un dispositivo se libera cuando un usuario o un atacante evitan diversas restricciones en un dispositivo para modificar el sistema operativo. Si selecciona este ajuste, los usuarios no pueden completar nuevas activaciones en un dispositivo con jailbreak, independientemente de la acción de cumplimiento que haya establecido.
Fallo de atestación de dispositivos gestionados	Esta configuración crea una regla de conformidad que especifica las acciones que se producen cuando un dispositivo no supera la atestación de dispositivos gestionados.
La aplicación no asignada está instalada	Esta configuración crea una regla de conformidad para garantizar que los dispositivos no tienen aplicaciones instaladas que no se asignaron al usuario. Esta configuración no se aplica a los dispositivos con el tipo de activación Privacidad del usuario.
La aplicación obligatoria no está instalada	Esta configuración crea una regla de conformidad para garantizar que los dispositivos tienen las aplicaciones necesarias instaladas.
Versión de SO restringida instalada	Esta configuración crea una regla de conformidad para garantizar que los dispositivos no tienen una versión de SO restringida instalada. Puede seleccionar las versiones del SO restringidas. Si selecciona este ajuste, los usuarios no pueden realizar nuevas activaciones para los dispositivos que no cumplan con los requisitos, independientemente de la acción de cumplimiento que haya establecido.
Modelo de dispositivo restringido detectado	Esta configuración crea una regla de conformidad para restringir modelos de dispositivo. Puede seleccionar los modelos de los dispositivos que están permitidos o restringidos. Si selecciona este ajuste, los usuarios no pueden realizar nuevas activaciones para los dispositivos que no cumplan con los requisitos, independientemente de la acción de cumplimiento que haya establecido.
Actualización del SO no aplicada	Esta configuración crea una regla de conformidad para ejecutar acciones de conformidad si un usuario no aplica una actualización pendiente del SO dentro de un periodo de tiempo que especifique.
Dispositivo fuera de contacto	Esta configuración crea una regla de conformidad para garantizar que los dispositivos no están fuera de contacto con UEM durante más de un periodo especificado. Especifique el número de días que un dispositivo puede estar sin contacto con UEM antes de que se considere fuera de conformidad.
Verificación de versiones de bibliotecas de BlackBerry Dynamics	Esta configuración crea una regla de conformidad que le permite seleccionar las versiones de bibliotecas de BlackBerry Dynamics que no se pueden activar. Puede seleccionar las versiones de bibliotecas bloqueadas.

Configuración del perfil de conformidad	Descripción
Verificación de la conectividad de BlackBerry Dynamics	Esta configuración crea una regla de conformidad para supervisar que las aplicaciones de BlackBerry Dynamics están fuera de contacto con UEM durante más tiempo del periodo especificado. La acción de cumplimiento se aplica a las aplicaciones de BlackBerry Dynamics. En la configuración "Basar intervalo de conectividad en las aplicaciones delegadas de la autenticación" se especifica que la verificación de conectividad se basa en el momento en el que se conecta una aplicación delegada de la autenticación a UEM. Esta configuración solo se aplica si se especifica un delegado de autenticación en un perfil de BlackBerry Dynamics. En la configuración "Hora del último contacto" se especifica el número de días que un dispositivo puede permanecer sin contacto con UEM antes de que se considere que el dispositivo infringe el cumplimiento. Las aplicaciones de BlackBerry Dynamics no solicitan a los usuarios el cumplimiento de esta regla. Si en "Comportamiento de solicitud" selecciona la opción "Aviso sobre conformidad", no se hará ninguna solicitud al usuario. Si el dispositivo puede ponerse en contacto con UEM, el dispositivo volverá a cumplir los requisitos cuando el usuario abra la aplicación de BlackBerry Dynamics.
Detección de capturas de pantalla de BlackBerry Dynamics en dispositivos iOS	**Nota:** La regla de conformidad anterior ha sido sustituida por la opción "No permitir capturas de pantalla en dispositivos iOS" en los perfiles de BlackBerry Dynamics. BlackBerry recomienda utilizar la configuración del perfil y desactivar esta regla de conformidad. Esta regla de conformidad quedará en desuso en una futura versión de UEM. Esta configuración crea una regla de cumplimiento que reacciona a las capturas de pantalla de las aplicaciones BlackBerry Dynamics en los dispositivos. En la configuración "Número máximo de capturas de pantalla en un periodo" se especifica el número de capturas de pantalla permitidas en el tiempo especificado. En el ajuste "Acción de conformidad para las aplicaciones de BlackBerry Dynamics" se especifica la acción que se produce si el usuario supera el número permitido de capturas de pantalla.

Configuración del perfil de conformidad	Descripción
La aplicación restringida está instalada	Esta configuración crea una regla de conformidad para que UEM compruebe periódicamente si hay aplicaciones restringidas, incluidas las aplicaciones del mercado. Añada aplicaciones a la lista de aplicaciones restringidas del perfil seleccionando las aplicaciones en la lista de aplicaciones restringidas de UEM o seleccionando una aplicación integrada (solo dispositivos supervisados). Cuando se selecciona esta configuración y hay instalada una aplicación restringida en un dispositivo, se muestra un mensaje de advertencia y un enlace en la pantalla Dispositivos gestionados de la consola. Al hacer clic en el enlace, se muestra una lista de las aplicaciones que hacen que el dispositivo no cumpla los requisitos de conformidad. La lista de aplicaciones restringidas también se envía al usuario en la notificación de conformidad. Para dispositivos supervisados, las acciones de cumplimiento para esta regla no son aplicables. Se impide automáticamente que los usuarios instalen aplicaciones restringidas. Si ya están instaladas aplicaciones restringidas (tanto incorporadas como instaladas por el usuario), estas aplicaciones se eliminarán automáticamente del dispositivo.
Mostrar solo las aplicaciones permitidas en el dispositivo	Esta configuración crea una regla de cumplimiento que especifica una lista de aplicaciones que pueden instalarse en los dispositivos, incluidas las aplicaciones del mercado. El resto de aplicaciones no están permitidas. Añada aplicaciones a la lista de aplicaciones permitidas del perfil seleccionando aplicaciones de la lista de aplicaciones UEM o seleccionando aplicaciones integradas. Algunas aplicaciones están incluidas en la lista de permitidos de manera predeterminada. Esta configuración solo es válida para dispositivos supervisados con .

macOS: configuración del perfil de conformidad

Consulte Común: configuración del perfil de conformidad para obtener una explicación sobre las acciones de cumplimiento que BlackBerry UEM puede llevar a cabo si un dispositivo infringe una regla de conformidad.

Configuración del perfil de conformidad	Descripción
Versión de SO restringida instalada	Esta configuración crea una regla de conformidad para garantizar que los dispositivos no tienen una versión de SO restringida instalada. Puede seleccionar las versiones del SO restringidas. Si selecciona este ajuste, los usuarios no pueden realizar nuevas activaciones para los dispositivos que no cumplan con los requisitos, independientemente de la acción de cumplimiento que haya establecido.

Configuración del perfil de conformidad	Descripción
Modelo de dispositivo restringido detectado	Esta configuración crea una regla de conformidad para restringir modelos de dispositivo. Puede seleccionar los modelos de los dispositivos que están permitidos o restringidos. Si selecciona este ajuste, los usuarios no pueden realizar nuevas activaciones para los dispositivos que no cumplan con los requisitos, independientemente de la acción de cumplimiento que haya establecido.
Verificación de versiones de bibliotecas de BlackBerry Dynamics	Esta configuración crea una regla de conformidad que le permite seleccionar las versiones de bibliotecas de BlackBerry Dynamics que no se pueden activar. Puede seleccionar las versiones de bibliotecas bloqueadas.
Verificación de la conectividad de BlackBerry Dynamics	Esta configuración crea una regla de conformidad para supervisar que las aplicaciones de BlackBerry Dynamics están fuera de contacto con UEM durante más tiempo del periodo especificado. La acción de cumplimiento se aplica a las aplicaciones de BlackBerry Dynamics. En la configuración "Basar intervalo de conectividad en las aplicaciones delegadas de la autenticación" se especifica que la verificación de conectividad se basa en el momento en el que se conecta una aplicación delegada de la autenticación a UEM. Esta configuración solo se aplica si se especifica un delegado de autenticación en un perfil de BlackBerry Dynamics. En la configuración "Hora del último contacto" se especifica el número de días que un dispositivo puede permanecer sin contacto con UEM antes de que se considere que el dispositivo infringe el cumplimiento.

Android: configuración del perfil de conformidad

Consulte Común: configuración del perfil de conformidad para obtener una explicación sobre las acciones de cumplimiento que BlackBerry UEM puede llevar a cabo si un dispositivo infringe una regla de conformidad.

Configuración del perfil de conformidad	Descripción
Atestación con errores de Knox o con rooting de SO	Esta configuración crea una regla de conformidad que especifica las acciones que se producen si un usuario o atacante obtiene acceso a la raíz de un dispositivo Android. Si selecciona este ajuste, los usuarios no podrán realizar nuevas activaciones para dispositivos con acceso a la raíz, independientemente de la acción de conformidad que haya establecido. Al seleccionar "Activar la detección de depuradores y emuladores cuando se ejecutan aplicaciones de BlackBerry Dynamics", se detienen las aplicaciones de BlackBerry Dynamics si el tiempo de ejecución de BlackBerry Dynamics detecta una herramienta de depuración o emulación activa. Si selecciona "Activar la detección de dispositivos de arranque desbloqueados o no verificados para aplicaciones de BlackBerry Dynamics", UEM podrá comprobar el estado de arranque del dispositivo.
Error de atestación de SafetyNet o Play Integrity	Esta configuración crea una regla de conformidad que especifica las acciones que se producen si los dispositivos no superan la atestación de SafetyNet o Play Integrity. Al utilizar la atestación de SafetyNet o Play Integrity, UEM envía comprobaciones para probar la autenticidad y la integridad de los dispositivos y aplicaciones Android de su entorno empresarial. Consulte Configuración de atestaciones de dispositivos Android y aplicaciones de BlackBerry Dynamics.
La aplicación no asignada está instalada	Esta configuración crea una regla de conformidad para garantizar que los dispositivos no tienen aplicaciones instaladas que no se asignaron al usuario. Cuando se selecciona esta configuración y hay instalada una aplicación no asignada en un dispositivo Android, se muestra un mensaje de advertencia y un enlace en la pantalla Dispositivos gestionados de la consola. Al hacer clic en el enlace, se muestra una lista de aplicaciones no asignadas. Para los dispositivos Android Enterprise, Android Management y Samsung Knox, los usuarios no pueden instalar aplicaciones no asignadas en el espacio de trabajo. Las acciones de conformidad no se aplican. Esta configuración no es válida para dispositivos activados con Privacidad del usuario.
La aplicación obligatoria no está instalada	Esta configuración crea una regla de conformidad para garantizar que los dispositivos tienen las aplicaciones necesarias instaladas. Cuando se selecciona esta opción y no hay instalada una aplicación necesaria en un dispositivo Android, se muestra un mensaje de advertencia y un enlace en la pantalla Dispositivos gestionados de la consola. Para los dispositivos Android Enterprise y Android Management, las acciones de cumplimiento no se aplican. Para los dispositivos con Samsung Knox, las aplicaciones internas requeridas se instalan automáticamente. Las acciones de conformidad solo se aplicarán a las aplicaciones públicas obligatorias.

Configuración del perfil de conformidad	Descripción
Versión de SO restringida instalada	Esta configuración crea una regla de conformidad para garantizar que los dispositivos no tienen una versión de SO restringida instalada. Puede seleccionar las versiones del SO restringidas. Si selecciona este ajuste, los usuarios no podrán realizar nuevas activaciones para los dispositivos que no cumplan con los requisitos, independientemente de la acción de conformidad que haya establecido.
Modelo de dispositivo restringido detectado	Esta configuración crea una regla de conformidad para restringir modelos de dispositivo. Puede especificar los modelos de los dispositivos que están permitidos o restringidos. Si selecciona este ajuste, los usuarios no podrán realizar nuevas activaciones para los dispositivos que no cumplan con los requisitos, independientemente de la acción de conformidad que haya establecido.
Actualización del SO no aplicada	Esta configuración crea una regla de conformidad para ejecutar acciones de conformidad si un usuario no aplica una actualización pendiente del SO dentro de un periodo de tiempo que especifique.
Dispositivo fuera de contacto	Esta configuración crea una regla de conformidad para supervisar si los dispositivos están fuera de contacto con UEM durante más tiempo del periodo especificado. En la configuración "Hora del último contacto" se especifica el número de días en los que un dispositivo puede estar fuera de contacto con UEM antes de que el dispositivo infrinja el cumplimiento.
El nivel de revisión de seguridad necesario no está instalado	Esta configuración crea una regla de conformidad para garantizar que los dispositivos tienen los parches de seguridad necesarios instalados. Puede especificar los modelos de dispositivo que deben tener parches de seguridad instalados y una fecha de parche de seguridad. Los dispositivos que ejecutan una revisión de seguridad igual o posterior a la fecha de la revisión de seguridad especificada se consideran conformes. Tras una actualización, si previamente ha creado un perfil de conformidad con el ajuste "El nivel de revisión de seguridad requerido no está instalado" activado, la acción de conformidad se establecerá en "Supervisar y registrar".
Verificación de versiones de bibliotecas de BlackBerry Dynamics	Esta configuración crea una regla de conformidad que le permite seleccionar las versiones de bibliotecas de BlackBerry Dynamics que no se pueden activar. Puede seleccionar las versiones de bibliotecas bloqueadas.

Configuración del perfil de conformidad	Descripción
Verificación de la conectividad de BlackBerry Dynamics	Esta configuración crea una regla de conformidad para supervisar que las aplicaciones de BlackBerry Dynamics están fuera de contacto con UEM durante más tiempo del periodo especificado. La acción de cumplimiento se aplica a las aplicaciones de BlackBerry Dynamics. En la configuración "Basar intervalo de conectividad en las aplicaciones delegadas de la autenticación" se especifica que la verificación de conectividad se basa en el momento en el que se conecta una aplicación delegada de la autenticación a UEM. Esta configuración solo se aplica si se especifica un delegado de autenticación en un perfil de BlackBerry Dynamics asignado. En la configuración "Hora del último contacto" se especifica el número de días que un dispositivo puede estar sin contacto con UEM antes de que se considere que infringe el cumplimiento.
La aplicación restringida está instalada	Esta configuración crea una regla de conformidad para garantizar que los dispositivos no tienen las aplicaciones restringidas instaladas. Para restringir aplicaciones, consulte Adición de una aplicación a la lista de aplicaciones restringidas. Para los dispositivos Android Enterprise y Android Management, los usuarios no pueden instalar aplicaciones restringidas en el espacio de trabajo. Las acciones de conformidad no se aplican. Para los dispositivos Samsung Knox, las aplicaciones restringidas en el espacio de trabajo se desactivan automáticamente. Las acciones de conformidad no se aplican. Para los dispositivos con el tipo de activación Trabajo y personal: control total (Samsung Knox), seleccione "Aplicar acciones de cumplimiento en el espacio personal" para aplicar la regla a las aplicaciones tanto en el perfil de trabajo como en el perfil personal. Esta configuración no es válida para dispositivos activados con Privacidad del usuario. Cuando se selecciona esta configuración y hay instalada una aplicación restringida en un dispositivo Android, se muestra un mensaje de advertencia y un enlace en la pestaña Dispositivos gestionados de la consola. Al hacer clic en el enlace, se muestra una lista de aplicaciones restringidas.
La contraseña no cumple los requisitos de complejidad	Esta configuración crea una regla de cumplimiento para garantizar que el usuario ha establecido contraseñas de dispositivo o espacio de trabajo que cumplen los requisitos de complejidad definidos en la política de TI asignada.

Windows: configuración del perfil de conformidad

Consulte Común: configuración del perfil de conformidad para obtener una explicación sobre las acciones de cumplimiento que BlackBerry UEM puede llevar a cabo si un dispositivo infringe una regla de conformidad.

Configuración del perfil de conformidad	Descripción
La aplicación obligatoria no está instalada	Esta configuración crea una regla de conformidad para garantizar que los dispositivos tienen las aplicaciones necesarias instaladas. Las disposiciones de las aplicaciones internas no pueden controlarse.
Versión de SO restringida instalada	Esta configuración crea una regla de conformidad para garantizar que los dispositivos no tienen una versión de SO restringida instalada. Puede seleccionar las versiones del SO restringidas.
Modelo de dispositivo restringido detectado	Esta configuración crea una regla de conformidad para restringir modelos de dispositivo. Puede seleccionar los modelos de los dispositivos que están permitidos o restringidos.
Dispositivo fuera de contacto	Esta configuración crea una regla de conformidad para garantizar que los dispositivos no están fuera de contacto con UEM durante más de un periodo especificado.
Verificación de versiones de bibliotecas de BlackBerry Dynamics	Esta configuración crea una regla de conformidad que le permite seleccionar las versiones de bibliotecas de BlackBerry Dynamics que no se pueden activar. Puede seleccionar las versiones de bibliotecas bloqueadas.
Verificación de la conectividad de BlackBerry Dynamics	Esta configuración crea una regla de conformidad para garantizar que las aplicaciones de BlackBerry Dynamics no están fuera de contacto con UEM durante más de un periodo especificado. La acción de cumplimiento se aplica a las aplicaciones de BlackBerry Dynamics.
Firma de antivirus	Esta configuración crea una regla de conformidad para garantizar que los dispositivos tienen una firma de antivirus activada.
Estado del antivirus	Esta configuración crea una regla de conformidad para garantizar que los dispositivos tienen el software antivirus activado. Puede seleccionar los proveedores permitidos.
Estado del firewall	Esta configuración crea una regla de conformidad para garantizar que los dispositivos tienen un firewall activado.
Estado del cifrado	Esta configuración crea una regla de conformidad para garantizar que los dispositivos requieren cifrado.
Estado de actualización de Windows	Esta configuración crea una regla de conformidad para garantizar que los dispositivos permiten a UEM instalar actualizaciones del sistema operativo Windows o notificar a los usuarios las actualizaciones necesarias.
La aplicación restringida está instalada	Esta configuración crea una regla de conformidad para garantizar que los dispositivos no tienen las aplicaciones restringidas instaladas. Para restringir aplicaciones, consulte Adición de una aplicación a la lista de aplicaciones restringidas.
Atestación del estado del dispositivo Windows	

Configuración del perfil de conformidad	Descripción
Periodo de gracia caducado	Esta configuración crea una regla de conformidad que le permite especificar las acciones que se llevan a cabo si se agota el periodo de gracia de la atestación.
Clave de identidad de la atestación no existente	Esta configuración crea una regla de conformidad que le permite especificar las acciones que se llevan a cabo si no hay una AIK presente en el dispositivo.
La política Prevención de ejecución de datos está desactivada	Esta configuración crea una regla de conformidad que le permite especificar las acciones que se llevan a cabo si la política DEP está desactivada en el dispositivo.
BitLocker está desactivado	Esta configuración crea una regla de conformidad que le permite especificar las acciones que se llevan a cabo si BitLocker está desactivado en el dispositivo.
El arranque seguro está desactivado	Esta configuración crea una regla de conformidad que le permite especificar las acciones que se llevan a cabo si el arranque seguro está desactivado en el dispositivo.
La integridad del código está desactivada	Esta configuración crea una regla de conformidad que le permite especificar las acciones que se llevan a cabo si la función de integridad del código está desactivada en el dispositivo.
El dispositivo está en modo seguro	Esta configuración crea una regla de conformidad que le permite especificar las acciones que se llevan a cabo si el dispositivo está en modo seguro.
El dispositivo está en el entorno de preinstalación de Windows	Esta configuración crea una regla de conformidad que le permite especificar las acciones que se llevan a cabo si el dispositivo está en el entorno de preinstalación de Windows.
El controlador antimalware de inicio temprano no está cargado	Esta configuración crea una regla de conformidad que le permite especificar las acciones que se llevan a cabo si el controlador antimalware de inicio temprano no está cargado.
El modo seguro virtual está desactivado	Esta configuración crea una regla de conformidad que le permite especificar las acciones que se llevan a cabo si el modo seguro virtual está desactivado.
La depuración de arranque está activada	Esta configuración crea una regla de conformidad que le permite especificar las acciones que se llevan a cabo si la depuración de arranque está activada.
La depuración del kernel del SO está activada	Esta configuración crea una regla de conformidad que le permite especificar las acciones que se llevan a cabo si el kernel del SO está activado.
La firma de pruebas está activada	Esta configuración crea una regla de conformidad que le permite especificar las acciones que se llevan a cabo si la firma de pruebas está activada.
La lista de revisiones del administrador de arranque no tiene la versión esperada	Esta configuración crea una regla de conformidad que le permite especificar las acciones que se llevan a cabo si la lista de revisiones del administrador de arranque no tiene la versión esperada. Especifique la versión esperada.

Configuración del perfil de conformidad	Descripción
La lista de revisiones de la integridad de código no tiene la versión esperada	Esta configuración crea una regla de conformidad que le permite especificar las acciones que se llevan a cabo si la lista de revisiones de la integridad de código no tiene la versión esperada. Especifique la versión esperada.
El hash de la política Integridad de código está presente y no tiene un valor permitido	Esta configuración crea una regla de conformidad que le permite especificar las acciones que se llevan a cabo si el hash de la política Integridad de código no está presente y no tiene un valor permitido. Especifique los valores permitidos.
El hash de la política de configuración de arranque seguro personalizado está presente y no tiene un valor permitido	Esta configuración crea una regla de conformidad que le permite especificar las acciones que se llevan a cabo si el hash de la política de configuración de arranque seguro personalizado no está presente y no tiene un valor permitido. Especifique los valores permitidos.
El valor de PCR no es un valor permitido	Esta configuración crea una regla de conformidad que le permite especificar las acciones que se llevan a cabo si el valor de PCR no es un valor permitido. Especifique los valores permitidos.

Supervisión de los eventos de conformidad

Después de configurar y asignar los perfiles de conformidad a los usuarios, puede usar la pantalla de eventos de conformidad para supervisar y realizar un seguimiento de las infracciones de conformidad en los dispositivos iOS, Android, macOS y Windows de los usuarios. En esta pantalla también se mostrarán los eventos de conformidad relacionados con las funciones de CylancePROTECT Mobile para UEM.

Antes de empezar: Crear y asignar perfiles de conformidad.

1. En la barra de menús de la consola de administración, haga clic en **Usuarios > Infracciones de la conformidad**.
2. Efectúe una de las acciones siguientes:
   - De forma predeterminada, esta pantalla muestra los nuevos eventos de conformidad del intervalo de fechas indicado. Para ver las alertas resueltas, ignoradas o todas, o para cambiar el intervalo de fechas, haga clic en **Editar**. Establezca el estado y el intervalo de fechas, y haga clic en **Enviar**.
   - En la sección **Filtros**, establezca los filtros adecuados para los eventos de conformidad que quiere ver y haga clic en **Enviar**.
   - Haga clic en ⋮ para establecer las columnas que desea mostrar.
   - Haga clic en una columna para ordenar los eventos según ese criterio.
   - Utilice el campo de búsqueda para buscar eventos de conformidad específicos.
3. Si desea eliminar un evento de esta vista, seleccione el evento y haga clic en ⊘. Al ignorar un evento, se elimina de esta vista sin que afecte al estado de conformidad del dispositivo asociado.
4. Para exportar eventos seleccionados a un archivo .csv, seleccione los eventos y haga clic en ➔.

Tenga en cuenta que los eventos de conformidad con cualquier estado se eliminan automáticamente de esta vista después de 120 días. Los eventos con un estado ignorado o resuelto se eliminan automáticamente después de 7 días.

Envío de comandos para los usuarios y dispositivos

Puede enviar varios comandos para gestionar las cuentas y los dispositivos de los usuarios. La lista de comandos que están disponibles depende del tipo de dispositivo y el tipo de activación. Puede enviar comandos a un usuario o dispositivo específico, o bien enviar comandos a varios usuarios y dispositivos mediante comandos masivos.

Por ejemplo, puede utilizar los comandos en las siguientes circunstancias:

- Si un dispositivo se pierde temporalmente, puede enviar un comando para bloquear el dispositivo o eliminar los datos de trabajo del dispositivo.
- Si desea redistribuir un dispositivo a otro usuario, puede enviar un comando para borrar todos los datos del dispositivo.
- Cuando un empleado deja la empresa, puede enviar un comando al dispositivo personal del usuario para eliminar solo los datos de trabajo.
- Si un usuario olvida la contraseña del espacio de trabajo, puede enviar un comando para restablecer la contraseña del espacio de trabajo.
- Para los usuarios con dispositivos supervisados de DEP, puede enviar un comando para activar una actualización del SO.

Envío de comandos a usuarios y dispositivos

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:

Tarea	Pasos
Enviar un comando a un usuario o dispositivo específico	**a.** Busque un usuario y haga clic en él. **b.** En la pestaña Dispositivo, en la sección **Gestionar dispositivo**, haga clic en el comando correspondiente.
Enviar un comando masivo a varios usuarios o dispositivos	**a.** Busque varios usuarios y selecciónelos. **b.** En el menú de comandos situado encima de la lista de usuarios, haga clic en el comando adecuado.

Para obtener más información sobre los comandos disponibles, consulte lo siguiente:

- Comandos para dispositivos con iOS y iPadOS.
- Comandos para dispositivos macOS.
- Comandos para dispositivos Android.
- Comandos para dispositivos Windows.

Después de terminar: Si desea establecer un periodo de caducidad para los comandos Eliminar todos los datos del dispositivo y Eliminar solo los datos de trabajo, consulte Establecer un tiempo de caducidad para comandos.

Establecer un tiempo de caducidad para comandos

Cuando envía el comando "Eliminar todos los datos del dispositivo" o "Eliminar solo los datos de trabajo" a un dispositivo, este debe conectarse a BlackBerry UEM para que el comando se complete. Si el dispositivo no se puede conectar a UEM, el comando permanece en estado pendiente y el dispositivo no se elimina

de UEM a menos que se elimine manualmente. Opcionalmente, se puede configurar UEM para que elimine automáticamente los dispositivos cuando no se completan los mandos tras un tiempo especificado.

1. En la barra de menús de la consola de administración, haga clic en **Configuración > Configuración general > Caducidad del comando de eliminación**.
2. Para uno o ambos comandos, seleccione **Eliminar automáticamente el dispositivo si el comando caduca**.
3. En el campo **Caducidad del comando**, indique tras cuántos días desea que caduque el comando y se elimine automáticamente el dispositivo de UEM.
4. Haga clic en **Guardar**.

Comandos para dispositivos con iOS y iPadOS

Comando	Descripción	Tipos de activación
Ver informe del dispositivo	Este comando muestra información detallada acerca de un dispositivo. Puede exportar y guardar el informe del dispositivo.	Controles de MDM Privacidad del usuario
Ver acciones de dispositivo	Este comando muestra todas las acciones que están en curso en un dispositivo.	Controles de MDM Privacidad del usuario
Eliminar todos los datos del dispositivo	Este comando elimina toda la información de usuario y los datos de aplicaciones que el dispositivo guarda y devuelve el dispositivo a la configuración predeterminada de fábrica. Si el dispositivo no se puede conectar a BlackBerry UEM cuando envía este comando, puede cancelar el comando o eliminar el dispositivo de la consola. Si el dispositivo se conecta a UEM una vez que lo elimine, solo se eliminarán los datos de trabajo del dispositivo. Si envía el comando a dispositivos con iOS 17 o posterior, puede seleccionar la opción "Activar retorno al servicio" y seleccionar un perfil de Wi-Fi para asignarlo a los dispositivos y ayudar al usuario a configurar el dispositivo nuevamente después de eliminar los datos. Si se detecta información de eSIM en uno o más de los dispositivos seleccionados, se le pedirá que especifique si se debe conservar la información del plan de datos.	Controles de MDM
Eliminar solo los datos de trabajo	Este comando elimina datos de trabajo, incluidas las políticas de TI, los perfiles, las aplicaciones y los certificados que se encuentran en un dispositivo. Si el dispositivo no se puede conectar a UEM cuando envía este comando, puede cancelar el comando o eliminar el dispositivo de la consola. Si el dispositivo se conecta a UEM una vez que lo elimine, se eliminarán los datos de trabajo del dispositivo.	Controles de MDM Privacidad del usuario

Comando	Descripción	Tipos de activación
Bloquear dispositivo	Este comando bloquea un dispositivo. Apple añade "iPhone perdido" o "iPad perdido" al título del mensaje que especifique. El usuario debe escribir la contraseña del dispositivo para desbloquear el dispositivo. Cuando se envía este comando, el dispositivo se bloquea solo si existe una contraseña para el dispositivo. De lo contrario, no se realiza ninguna acción en el dispositivo. Este comando no es compatible con dispositivos Apple TV.	Controles de MDM
Desbloquear y borrar contraseña	Este comando desbloquea un dispositivo y elimina la contraseña. Al usuario se le indica que cree una contraseña para el dispositivo. Puede utilizar este comando si el usuario olvida la contraseña del dispositivo. Este comando no es compatible con dispositivos Apple TV.	Controles de MDM
Activar modo perdido	Este comando bloquea el dispositivo y le permite mostrar un número de teléfono y un mensaje en el dispositivo. Después de enviar este comando, podrá ver la ubicación del dispositivo desde la consola de administración. Este comando solo es compatible con dispositivos supervisados. Este comando no es compatible con dispositivos Apple TV.	Controles de MDM
Desactivar BlackBerry 2FA	Este comando desactiva los dispositivos que se activan con el tipo de activación BlackBerry 2FA. El dispositivo se elimina de UEM y el usuario no puede utilizar la característica BlackBerry 2FA. Este comando no es compatible con dispositivos Apple TV.	Controles de MDM
Actualizar SO	Este comando fuerza los dispositivos a instalar una actualización del SO. Este comando solo es compatible con dispositivos supervisados. Este comando no es compatible con dispositivos Apple TV.	Controles de MDM
Reiniciar dispositivo	Este comando fuerza al dispositivo a reiniciarse. Este comando solo es compatible con dispositivos supervisados. Este comando no es compatible con dispositivos Apple TV.	Controles de MDM
Desactivar dispositivo	Este comando fuerza al dispositivo a desactivarse. Este comando solo es compatible con dispositivos supervisados. Este comando no es compatible con dispositivos Apple TV.	Controles de MDM

Comando	Descripción	Tipos de activación
Limpiar aplicaciones	Este comando borra los datos de todas las aplicaciones gestionadas de Microsoft Intune en el dispositivo. Las aplicaciones no se eliminan del dispositivo.	Controles de MDM
Actualizar la información del dispositivo	Este comando envía y recibe información del dispositivo actualizada. Por ejemplo, puede enviar reglas de políticas de TI actualizadas recientemente o perfiles a un dispositivo y recibir información actualizada acerca de un dispositivo, como la versión del SO o el nivel de la batería.	Controles de MDM Privacidad del usuario
Actualizar zona horaria	Este comando establece la hora del dispositivo en función de la región que seleccione.	Controles de MDM
Eliminar dispositivo	Este comando elimina el dispositivo de UEM, pero no borra los datos del dispositivo. El dispositivo puede seguir recibiendo correos electrónicos y otros datos de trabajo. Este comando está destinado para los dispositivos que se hayan dañado o perdido de forma irreversible y no se espere que vuelvan a contactar con el servidor. Si un dispositivo que se haya eliminado intenta contactar con UEM, el usuario recibe una notificación y el dispositivo no podrá comunicarse con UEM a menos que se reactive.	Controles de MDM Privacidad del usuario
Actualizar eSIM	Para dispositivos que tienen un plan de telefonía móvil basado en eSIM, este comando consulta los detalles del plan actualizado para el dispositivo desde la URL del operador del dispositivo.	Controles de MDM

Comandos para dispositivos macOS

Comando	Descripción
Ver informe del dispositivo	Este comando muestra información detallada acerca de un dispositivo. Puede exportar y guardar el informe del dispositivo.
Ver acciones de dispositivo	Este comando muestra todas las acciones que están en curso en un dispositivo.
Bloquear escritorio	Este comando le permite establecer un PIN y bloquear el dispositivo.
Eliminar solo los datos de trabajo	Este comando elimina datos de trabajo, incluida la política de TI, los perfiles, las aplicaciones y los certificados que se encuentran en el dispositivo y, opcionalmente, elimina el dispositivo de BlackBerry UEM.

Comando	Descripción
Eliminar todos los datos del dispositivo	Este comando elimina toda la información del usuario y los datos de aplicaciones del dispositivo. Devuelve el dispositivo a los valores predeterminados de fábrica, lo bloquea con el PIN que establezca y, opcionalmente, elimina el dispositivo de UEM.
Actualizar datos de escritorio	Este comando envía y recibe información del dispositivo actualizada. Por ejemplo, puede enviar reglas de políticas de TI actualizadas recientemente o perfiles a un dispositivo y recibir información actualizada acerca de un dispositivo, como la versión del SO o el nivel de la batería.
Eliminar dispositivo	Este comando elimina el dispositivo de UEM. El dispositivo puede seguir recibiendo correos electrónicos y otros datos de trabajo.

Comandos para dispositivos Android

Para obtener información sobre los tipos de activación de Android Management, consulte Consideraciones sobre los tipos de activación de Android Management.

Comando	Descripción	Tipos de activación
Ver informe del dispositivo	Este comando muestra información detallada acerca de un dispositivo. Puede exportar y guardar el informe del dispositivo.	Todos (excepto BlackBerry 2FA)
Ver acciones de dispositivo	Este comando muestra todas las acciones que están en curso en un dispositivo.	Todos (excepto BlackBerry 2FA)
Bloquear dispositivo	Este comando bloquea el dispositivo. El usuario debe escribir la contraseña del dispositivo para desbloquear el dispositivo. Cuando se envía este comando, el dispositivo se bloquea solo si existe una contraseña para el dispositivo. De lo contrario, no se realiza ninguna acción en el dispositivo.	Trabajo y personal: control total (Android Management) Trabajo y personal: privacidad de usuario (Android Management) Solo espacio de trabajo (Android Management) Trabajo y personal: control total (Android Enterprise) Trabajo y personal: privacidad de usuario (Android Enterprise) Solo espacio de trabajo (Android Enterprise) Controles de MDM

Comando	Descripción	Tipos de activación
Eliminar todos los datos del dispositivo	Este comando elimina toda la información del usuario y los datos de aplicaciones que almacena el dispositivo, incluida la información en el espacio de trabajo, y devuelve el dispositivo a la configuración predeterminada de fábrica. Si el dispositivo no se puede conectar a UEM cuando envía este comando, puede cancelar el comando o eliminar el dispositivo de la consola. Si el dispositivo se conecta a UEM una vez que lo elimine, solo se eliminarán los datos de trabajo del dispositivo, incluido el espacio de trabajo, si procede.	Trabajo y personal: control total (Android Management) Solo espacio de trabajo (Android Management) Trabajo y personal: control total (Android Enterprise) Trabajo y personal: control total (Samsung Knox) Controles de MDM
Eliminar solo los datos de trabajo	Este comando elimina datos de trabajo, incluida la política de TI, los perfiles, aplicaciones y certificados que se encuentran en el dispositivo y desactiva el dispositivo. Si el dispositivo tiene un espacio de trabajo, el espacio de trabajo se elimina del dispositivo, pero se conservan todas las aplicaciones y datos personales. Cuando utiliza este comando en dispositivos con Android Enterprise, puede escribir un motivo para que aparezca en la notificación del dispositivo del usuario para explicar por qué se borró el perfil de trabajo. Si el dispositivo no se puede conectar a UEM cuando envía este comando, puede cancelar el comando o eliminar el dispositivo de la consola. Si el dispositivo se conecta a UEM una vez que lo haya eliminado, se eliminarán los datos de trabajo del dispositivo, incluido el espacio de trabajo, si procede.	Trabajo y personal: control total (Android Management) Trabajo y personal: privacidad de usuario (Android Management) Trabajo y personal: control total (Android Enterprise) Trabajo y personal: privacidad de usuario (Android Enterprise) Trabajo y personal: control total (Samsung Knox) Trabajo y personal: privacidad de usuario (Samsung Knox) Controles de MDM

Comando	Descripción	Tipos de activación
Desbloquear dispositivo y borrar contraseña	Este comando desbloquea el dispositivo y solicita al usuario que cree una nueva contraseña para el dispositivo. Si el usuario omite la pantalla "Crear contraseña de dispositivo" se conserva la contraseña anterior. Puede utilizar este comando si un usuario olvida la contraseña del dispositivo. Este comando no es compatible con dispositivos con Samsung Knox SDK 3.2.1 y posterior.	Trabajo y personal: control total (Samsung Knox) Trabajo y personal: privacidad de usuario (Samsung Knox) Controles de MDM (solo dispositivos Samsung)
Especificar la contraseña del dispositivo y bloquearlo	Este comando permite crear una contraseña del dispositivo y, a continuación, bloquear el dispositivo. Debe crear una contraseña que cumpla con las actuales reglas para la contraseña. Para desbloquear el dispositivo, el usuario debe escribir la nueva contraseña.	Trabajo y personal: privacidad de usuario (Android Management) Solo espacio de trabajo (Android Management) Solo espacio de trabajo (Android Enterprise) Trabajo y personal: control total (Samsung Knox)
Restablecer contraseña del espacio de trabajo	Este comando elimina la contraseña actual del espacio de trabajo del dispositivo. Cuando el usuario abre el espacio de trabajo, el dispositivo solicita al usuario que defina una nueva contraseña del espacio de trabajo.	Trabajo y personal: control total (Samsung Knox) Trabajo y personal: privacidad de usuario - (Samsung Knox)
Especificar contraseña de espacio de trabajo y bloquear	Este comando permite especificar una contraseña para el perfil de trabajo y bloquear el dispositivo. Cuando el usuario abre una aplicación de trabajo, debe introducir la contraseña que se especificó.	Trabajo y personal: control total (Android Enterprise) Trabajo y personal: privacidad de usuario (Android Enterprise)
Desactivar/activar espacio de trabajo	Este comando desactiva o activa el acceso a las aplicaciones del espacio de trabajo en el dispositivo.	Trabajo y personal: control total (Android Management) Trabajo y personal: privacidad de usuario (Android Management) Solo espacio de trabajo (Android Management) Trabajo y personal: control total (Samsung Knox) Trabajo y personal: privacidad de usuario - (Samsung Knox)

Comando	Descripción	Tipos de activación
Desactivar BlackBerry 2FA	Este comando desactiva los dispositivos que se activan con el tipo de activación BlackBerry 2FA. El dispositivo se elimina de UEM y el usuario no puede utilizar la característica BlackBerry 2FA.	BlackBerry 2FA
Limpiar aplicaciones	Este comando borra los datos de todas las aplicaciones gestionadas de Microsoft Intune en el dispositivo. Las aplicaciones no se eliminan del dispositivo.	Todas (excepto BlackBerry 2FA)
Actualizar la información del dispositivo	Este comando envía y recibe información del dispositivo actualizada. Por ejemplo, puede enviar perfiles o reglas de políticas de TI que se hayan actualizado recientemente a un dispositivo y recibir información actualizada acerca de un dispositivo, como la versión del SO o el nivel de batería.	Todos (excepto BlackBerry 2FA)
Solicitar informe de errores	Este comando envía una solicitud al dispositivo para los registros de cliente. El usuario de dispositivo debe aceptar o rechazar la solicitud.	Solo espacio de trabajo (Android Enterprise) Trabajo y personal: control total (Android Enterprise)
Reiniciar dispositivo	Este comando envía una solicitud al dispositivo para que se reinicie. En un mensaje se indica al usuario que el dispositivo se reiniciará en un minuto. El usuario de dispositivo tiene la opción de retrasar 10 minutos el reinicio.	Solo espacio de trabajo (Android Management) Solo espacio de trabajo (Android Enterprise)
Eliminar dispositivo	Este comando elimina el dispositivo de UEM, pero no borra los datos del dispositivo. El dispositivo puede seguir recibiendo correos electrónicos y otros datos de trabajo. Este comando está destinado para los dispositivos que se hayan dañado o perdido de forma irreversible y no se espere que vuelvan a contactar con el servidor. Si un dispositivo que se haya eliminado intenta contactar con UEM, el usuario recibe una notificación y el dispositivo no podrá comunicarse con UEM a menos que se reactive.	Todos (excepto BlackBerry 2FA)

Comandos para dispositivos Windows

Comando	Descripción
Ver informe del dispositivo	Este comando muestra información detallada acerca de un dispositivo. Puede exportar y guardar el informe del dispositivo.
Ver acciones de dispositivo	Este comando muestra todas las acciones que están en curso en un dispositivo.
Bloquear dispositivo	Este comando bloquea un dispositivo. El usuario debe escribir la contraseña del dispositivo para desbloquear el dispositivo. Cuando se envía este comando, el dispositivo se bloquea solo si existe una contraseña para el dispositivo. De lo contrario, no se realiza ninguna acción en el dispositivo. Este comando solo es compatible con dispositivos que ejecutan Windows 10 Mobile.
Generar contraseña de dispositivo y bloquear	Este comando crea una contraseña del dispositivo y bloquea el dispositivo. La contraseña generada se envía al usuario por correo. Puede utilizar la dirección de correo preseleccionada, o especificar una dirección de correo. La contraseña generada cumple con las reglas para la contraseña. Este comando solo es compatible con dispositivos que ejecutan Windows 10 Mobile.
Eliminar solo los datos de trabajo	Este comando elimina datos de trabajo, incluida la política de TI, los perfiles, las aplicaciones y los certificados que se encuentran en el dispositivo y, opcionalmente, elimina el dispositivo de BlackBerry UEM. La cuenta de usuario no se elimina al enviar este comando. Después de enviar este comando, se le dará la opción de eliminar el dispositivo de UEM. Si el dispositivo no se puede conectar a UEM, puede eliminarlo de UEM. Si el dispositivo se conecta a UEM una vez que lo haya eliminado, solo se eliminarán los datos de trabajo del dispositivo, incluido el espacio de trabajo, si procede.
Eliminar todos los datos del dispositivo	Este comando elimina toda la información del usuario y los datos de aplicaciones guardados en el dispositivo. Devuelve el dispositivo a los valores predeterminados de fábrica y, opcionalmente, lo elimina de UEM. Después de enviar este comando, se le dará la opción de eliminar el dispositivo de UEM. Si el dispositivo no se puede conectar a UEM, puede eliminarlo de UEM. Si el dispositivo se conecta a UEM una vez que lo haya eliminado, solo se eliminarán los datos de trabajo del dispositivo, incluido el espacio de trabajo, si procede.
Reinicie el escritorio o dispositivo	Este comando fuerza al dispositivo a reiniciarse.

Comando	Descripción
Actualizar la información del dispositivo	Este comando envía y recibe información del dispositivo actualizada. Por ejemplo, puede enviar perfiles o reglas de políticas de TI que se hayan actualizado recientemente a un dispositivo y recibir información actualizada acerca de un dispositivo, como la versión del SO o el nivel de batería. El comando también envía una solicitud al dispositivo para crear una solicitud de validación del certificado de estado. El dispositivo envía la solicitud al Servicio de atestación de mantenimiento de Microsoft para comprobar la conformidad. Esta función solo es compatible en un entorno local.
Eliminar dispositivo	Este comando elimina el dispositivo de UEM. El dispositivo puede seguir recibiendo correos electrónicos y otros datos de trabajo.

Control del modo en que se instalan las actualizaciones de software en los dispositivos

Puede utilizar los perfiles de requisitos de informe especial de los dispositivos para controlar cómo se instalan las actualizaciones de software de los dispositivos Android Enterprise, Android Management y Samsung Knox, y también cómo se administran las actualizaciones de aplicaciones para las aplicaciones que se ejecutan en primer plano.

Puede utilizar las reglas de políticas de TI para controlar las actualizaciones de software en dispositivos iOS. Para obtener más información, consulte la Hoja de cálculo de referencia de políticas de TI. También puede utilizar la consola de administración para actualizar el sistema operativo en dispositivos iOS supervisados.

Creación de un perfil de requisitos de informe especial para dispositivos Android Enterprise y Android Management

Las reglas de actualización del SO solo se aplican a los dispositivos Android Enterprise y Android Management con tipos de activación Solo espacio de trabajo y Trabajo y personal: control total. Estas reglas se aplican a todos los dispositivos Android Enterprise. Actualmente, los dispositivos Android Management no admiten la suspensión de las actualizaciones del sistema operativo ni las actualizaciones automáticas de las aplicaciones. Consulte Consideraciones sobre los tipos de activación de Android Management.

1. En la barra de menús de la consola de administración, haga clic en **Políticas y perfiles > Conformidad > Requisitos de informe especial del dispositivo**.
2. Haga clic en +.
3. Escriba un nombre y una descripción para el perfil.
4. Para configurar las reglas de actualización del SO para los dispositivos Solo espacio de trabajo y Trabajo y personal: control total y, en la sección **Regla de actualización del SO**, haga clic en + y haga lo siguiente:
   a) En la lista desplegable **Modelo de dispositivo**, seleccione un modelo de dispositivo.
   b) En la lista desplegable **Versión del SO**, seleccione la versión del sistema operativo.
   c) En la lista desplegable **Regla de actualización**, seleccione una de las siguientes opciones:
      - **Predeterminado**: el usuario puede elegir cuándo se instalan las actualizaciones. Los usuarios con el tipo de activación Solo espacio de trabajo (dispositivo totalmente gestionado) no pueden elegir cuándo instalar las actualizaciones.
      - **Actualizar automáticamente**: las actualizaciones se instalan sin preguntar al usuario.
      - **Actualizar automáticamente entre**: las actualizaciones se instalan en el intervalo de tiempo que especifique, sin preguntar al usuario. El usuario puede elegir que las actualizaciones se instalen fuera de este intervalo.
      - **Retrasar hasta 30 días**: bloquear la instalación de actualizaciones durante 30 días. Después de 30 días, el usuario puede elegir cuándo se instalan las actualizaciones. En del fabricante del dispositivo y el proveedor de servicios inalámbricos, puede que las actualizaciones de seguridad no se retrasen.
   d) Haga clic en **Agregar**.
5. Para especificar los periodos de tiempo en los que no deben producirse actualizaciones del sistema operativo para los dispositivos Solo espacio de trabajo y Trabajo y personal: control total, en la sección **Suspender actualizaciones del sistema operativo**, haga clic en +. Seleccione el mes y el día en que comienza el periodo de suspensión y la duración del periodo de suspensión.

   Si especifica más de un periodo de suspensión, debe haber al menos 60 días entre los periodos.

6. Para especificar un periodo de actualización para las aplicaciones que se ejecutan en primer plano, seleccione la opción **Activar el periodo de actualización para aplicaciones que se ejecutan en primer plano**. Seleccione la hora de inicio y la duración.
7. Para especificar cómo Google Play aplica los cambios a las aplicaciones que se ejecutan en primer plano (el ajuste Actualización automática de aplicaciones de Google Play), en la lista desplegable **Política de actualización automática de aplicaciones**, seleccione una de las siguientes opciones:

   - **Siempre**: las aplicaciones se actualizarán siempre. Tenga en cuenta que, para las aplicaciones que siempre están en ejecución, (por ejemplo, BlackBerry UEM Client, BlackBerry Work o BlackBerry Connectivity), si no selecciona la opción **Activar el periodo de actualización para aplicaciones que se ejecutan en primer plano**, la aplicación no se actualizará hasta que el usuario lo haga manualmente.
   - **Solo Wi-Fi**: las aplicaciones se actualizarán solamente cuando el dispositivo esté conectado a una red Wi-Fi. Tenga en cuenta que, para las aplicaciones que siempre están en ejecución, (por ejemplo, UEM Client, BlackBerry Work o BlackBerry Connectivity), si no selecciona la opción **Activar el periodo de actualización para aplicaciones que se ejecutan en primer plano**, la aplicación no se actualizará hasta que el usuario lo haga manualmente.
   - **El usuario puede permitir**: se pedirá al usuario que permita que se actualicen las aplicaciones del dispositivo.
   - **Desactivar**: las aplicaciones no se actualizarán nunca.

   Si selecciona **Siempre**, **Solo Wi-Fi** o **Desactivar**, el usuario no podrá seleccionar una opción diferente en el dispositivo. Los usuarios podrán seguir actualizando manualmente las aplicaciones en Google Play.
8. Haga clic en **Agregar**.

Después de terminar:

- Asigne el perfil a usuarios y grupos.
- Si es necesario, clasifique el perfil.
- Para ver una lista de los usuarios que están ejecutando una versión de software revocada (una versión de software que ya no acepta un proveedor de servicios), en **Políticas y perfiles > Cumplimiento > Requisitos de informe especial del dispositivo**, haga clic en un perfil y, a continuación, en **x usuarios con versión de informe especial rechazada**.

Crear un perfil de requisitos de solicitud de servicio del dispositivo para dispositivos con Samsung Knox

En los dispositivos con Samsung Knox, puede utilizar Knox E-FOTA One (Enterprise Firmware Over the Air) para controlar cuándo se instalan las actualizaciones de firmware de Samsung. Si su empresa utiliza Samsung E-FOTA (fin de servicio el 31 de julio de 2022) y necesita migrar a E-FOTA One, consulte KB 69901.

Los dispositivos Samsung Knox que se activan como Trabajo y personal: control total (Samsung Knox), Solo espacio de trabajo (dispositivo con Android Enterprise completamente gestionado) y Trabajo y personal: control total (dispositivo con Android Enterprise totalmente gestionado con perfil de trabajo) admiten restricciones de software mediante E-FOTA One.

E-FOTA One no es compatible con los tipos de activación de Trabajo y personal: privacidad de usuario (Samsung Knox) o Trabajo y personal: privacidad de usuario (Android Enterprise con perfil de trabajo).

Antes de empezar:

- En la barra de menús de la consola de administración, vaya a **Configuración > Resumen de licencias** para añadir una licencia de E-FOTA a BlackBerry UEM.
- Para utilizar E-FOTA, debe activar la regla global "Permitir actualizaciones OTA" de Android en la política de TI que asigne a los dispositivos.

1. En la barra de menús de la consola de administración, haga clic en **Políticas y perfiles > Conformidad > Requisitos de informe especial del dispositivo**.
2. Haga clic en +.
3. Escriba un nombre y una descripción para el perfil.
4. Si desea permitir que las reglas de actualización del sistema operativo Android se apliquen a los dispositivos Samsung, seleccione la casilla de verificación **Aplicar restricción a todos los dispositivos Android**.

   Las reglas de firmware que configurará en los siguientes pasos tendrán prioridad sobre estas reglas. Los ajustes de Suspender actualizaciones del SO no se aplican a los dispositivos Samsung Knox que utilizan E-FOTA.
5. En la sección **Reglas de firmware del dispositivo Samsung**, haga clic en +.
6. En la lista despegable **Modelo de dispositivo**, introduzca el modelo de dispositivo o seleccione uno en la lista.
7. En la lista desplegable **Idioma**, seleccione un idioma.
8. En el campo **Código del operador**, introduzca el código CSC del proveedor de servicios inalámbricos.
9. Haga clic en **Obtener versión de firmware**.
10. Repita los pasos anteriores para cada regla de firmware que desee añadir.
11. Cuando haya terminado, haga clic en **Agregar**.
12. Si desea programar una actualización forzada, haga clic en **Programar** junto a la versión de firmware que haya añadido. En el cuadro de diálogo **Programar actualización forzada**, haga lo siguiente:
    a) En los campos **Programar actualización forzada entre**, seleccione el intervalo de fechas en el que se debe instalar la actualización.
    b) En las listas desplegables **Programar actualización forzada durante las horas de**, especifique cuándo se debe instalar la actualización forzada.

    Si programa una actualización forzada, el dispositivo Knox ya no estará restringido a la versión del firmware y podrá actualizarlo manualmente si hay disponible una versión posterior.
13. Haga clic en **Guardar**.

Después de terminar:

- Asigne el perfil a usuarios y grupos.
- Si es necesario, clasifique el perfil.
- Para ver una lista de los usuarios que están ejecutando una versión de software revocada (una versión de software que ya no acepta un proveedor de servicios), en **Políticas y perfiles > Cumplimiento > Requisitos de informe especial del dispositivo**, haga clic en un perfil y, a continuación, en **x usuarios con versión de informe especial rechazada**.

Actualización del SO en dispositivos de iOS supervisados

Puede utilizar la consola de administración para forzar que los dispositivos iOS supervisados instalen una actualización del sistema operativo disponible.

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
Actualización del SO en dispositivos iOS supervisados específicos	**a.** Busque el nombre de una cuenta de usuario y haga clic en él. **b.** En la pestaña del dispositivo correspondiente, si hay una actualización de software disponible, haga clic en **Actualizar ahora**. **c.** Configure los ajustes de actualización del SO que corresponda. **d.** Haga clic en **Actualizar**.
Actualización del SO en varios dispositivos iOS supervisados	**a.** Seleccione las cuentas de usuario. **b.** Haga clic en . **c.** Configure los ajustes de actualización del SO que corresponda. **d.** Haga clic en **Actualizar**.

Configuración de cómo los dispositivos se ponen en contacto con BlackBerry UEM para actualizaciones de aplicaciones y configuraciones

El perfil Enterprise Management Agent se asegura de que los dispositivos se pongan en contacto periódicamente con BlackBerry UEM para actualizar las aplicaciones y la configuración. Cuando hay una actualización para un dispositivo, UEM solicita al dispositivo que se ponga en contacto con UEM para recibir actualizaciones. Si por algún motivo el dispositivo no recibe el aviso, se utiliza el perfil de Enterprise Management Agent para asegurarse de que el dispositivo se ponga en contacto con UEM en el intervalo que especifique.

En entornos locales, también puede utilizar el perfil Enterprise Management Agent para permitir que UEM pueda recopilar una lista de aplicaciones personales en los dispositivos de los usuarios.

Creación de un perfil de Enterprise Management Agent

1. En la barra de menús de la consola de administración, haga clic en **Políticas y perfiles > Política > Agente de Enterprise Management**.
2. Haga clic en +.
3. Escriba un nombre y una descripción para el perfil.
4. Configure los valores adecuados para cada tipo de dispositivo. Para más información sobre la configuración, consulte lo siguiente:
   - iOS: configuración del perfil de Enterprise Management Agent
   - Android: configuración del perfil de Enterprise Management Agent
   - Windows: configuración del perfil de Enterprise Management Agent
5. Haga clic en **Agregar**.

Después de terminar:

- Asigne el perfil a usuarios y grupos.
- Si es necesario, clasifique el perfil.

iOS: configuración del perfil de Enterprise Management Agent

Configuración	Descripción
Frecuencia de sondeo de Enterprise Management Agent	Especifique la frecuencia en segundos con que el dispositivo debe buscar comandos de servidor de Enterprise Management Agent. El dispositivo solo realiza búsquedas cuando UEM Client está abierto.
Permitir colecciones de aplicaciones personales	Especifique si BlackBerry UEM debe recibir una lista de las aplicaciones personales que están instaladas en el dispositivo de un usuario. Esta opción no es compatible con los dispositivos con activaciones de privacidad del usuario.

Android: configuración del perfil de Enterprise Management Agent

Configuración	Descripción
Cambios de la aplicación	Especifique con qué frecuencia, en segundos, desea que el dispositivo busque los cambios de las aplicaciones instaladas.
Umbral del nivel de batería	Especifique el cambio obligatorio en el porcentaje de nivel de batería para que el dispositivo envíe la información de nuevo a BlackBerry UEM.
Umbral de espacio libre de RAM	Especifique el cambio obligatorio en la cantidad de memoria libre en megabytes para que el dispositivo envíe la información de nuevo a UEM.
Umbral del almacenamiento interno	Especifique el cambio requerido en la cantidad de espacio de almacenamiento interno libre en megabytes antes de que el dispositivo envíe la información de nuevo a UEM.
Umbral de la tarjeta de memoria	Especifique el cambio obligatorio en la cantidad de espacio libre externo en megabytes para que el dispositivo envíe la información de nuevo a UEM.
Frecuencia de sondeo de Enterprise Management Agent	Especifique la frecuencia en segundos con que el dispositivo debe buscar comandos de servidor de Enterprise Management Agent.
Permitir colecciones de aplicaciones personales	Especifique si UEM debe recibir una lista de las aplicaciones personales que están instaladas en el dispositivo de un usuario. Esta opción no es compatible con los dispositivos con activaciones de privacidad del usuario.

Windows: configuración del perfil de Enterprise Management Agent

Configuración	Descripción
Intervalo de sondeo para las actualizaciones de configuración de los dispositivos	Especifique en minutos con qué frecuencia desea que el dispositivo busque actualizaciones cuando la notificación de inserción no esté disponible.
Intervalo de sondeo para el primer conjunto de reintentos	Especifique el tiempo en minutos que debe esperarse entre intentos para el primer conjunto de reintentos si falla la búsqueda de actualizaciones para la configuración del dispositivo.
Número de primeros reintentos	Especifique el número de intentos del primer conjunto de reintentos.
Intervalo de sondeo para el segundo conjunto de reintentos	Especifique el tiempo en minutos que debe esperarse entre intentos para el segundo conjunto de reintentos si falla la búsqueda de actualizaciones para la configuración del dispositivo.

Configuración	Descripción
Número de segundos reintentos	Especifique el número de intentos del segundo conjunto de reintentos.
Intervalo de sondeo de los reintentos programados restantes	Especifique el tiempo en minutos que debe esperarse entre los intentos sucesivos después del segundo conjunto de reintentos si falla la búsqueda de actualizaciones para la configuración del dispositivo.
Número de reintentos programados restantes	Especifique el número de intentos sucesivos después del segundo conjunto de reintentos si falla la búsqueda de actualizaciones para la configuración del dispositivo. Si se ajusta a "0", el dispositivo continuará realizando sondeos hasta que se establezca una conexión correctamente o hasta que se desactive el dispositivo.
Sondeo en inicio de sesión de usuario	Especifique si el dispositivo debe iniciar una sesión de administración siempre que un usuario inicie sesión.
Sondeo de todos los usuarios en el primer inicio de sesión	Especifique si el dispositivo debe iniciar una sesión de administración la primera vez que inicien sesión todos los usuarios.
Permitir colecciones de aplicaciones personales	Especifique si BlackBerry UEM debe recibir una lista de las aplicaciones personales que están instaladas en el dispositivo de un usuario.

Presentación de la información de la empresa en los dispositivos

Puede configurar BlackBerry UEM para mostrar la información de la empresa y avisos de empresa personalizados en los dispositivos.

Para los dispositivos iOS, macOS, Android y Windows 10, puede crear avisos personalizados para la empresa que se mostrarán durante el proceso de activación (por ejemplo, puede mostrar un aviso sobre las condiciones que debe seguir un usuario para cumplir con los requisitos de seguridad de la empresa). El usuario debe aceptar el aviso para continuar con el proceso de activación. Puede crear varios avisos y versiones separadas de cada aviso para admitir diferentes idiomas.

Puede crear perfiles de dispositivo para mostrar información sobre la empresa en los dispositivos. En los dispositivos iOS y Android, la información de la empresa se muestra en BlackBerry UEM Client. En Windows 10, el número de teléfono y la dirección de correo se muestran en la información de soporte en el dispositivo. En los dispositivos con Samsung Knox, puede utilizar el perfil de dispositivo para mostrar el aviso de empresa personalizado cuando el usuario reinicia el dispositivo.

En los dispositivos supervisados con Samsung Knox y iOS, también puede utilizar el perfil de dispositivo para añadir una imagen de fondo de pantalla personalizada con la información que se debe mostrar a los usuarios. Por ejemplo, puede crear una imagen que contenga la información de asistencia y contacto, la información interna de la página web o el logotipo de la empresa. En los dispositivos con Samsung Knox, el fondo de pantalla se muestra en el espacio de trabajo.

Los perfiles de dispositivos no son compatibles con dispositivos con iOS que se activan con un tipo de activación de privacidad de usuario.

Crear avisos de la empresa

1. En la barra de menús de la consola de administración, haga clic en **Configuración > Configuración general > Avisos de la empresa**.
2. Haga clic en +.
3. Escriba un nombre para el aviso de la empresa.
4. Opcionalmente, puede reutilizar el texto de otro aviso de la empresa si lo selecciona en la lista desplegable **Texto copiado del aviso de la empresa**.
5. En la lista desplegable **Idioma del dispositivo**, seleccione el idioma predeterminado para el aviso.
6. En el campo **Aviso de la empresa**, escriba el texto del aviso.
7. Opcionalmente, puede hacer clic en **Agregar un idioma adicional** las veces que haga falta para publicar el aviso de la empresa en más idiomas.
8. Si publica el aviso de la empresa en más de un idioma, seleccione la opción **Idioma predeterminado** debajo de uno de los mensajes para convertirlo en el idioma predeterminado.
9. Haga clic en **Guardar**.

Después de terminar:

- Para mostrar el aviso de la empresa durante la activación, asigne el aviso de la empresa a un perfil de activación.
- Para mostrar el aviso de la empresa cuando se reinicie un dispositivo con Samsung Knox, asigne el aviso de la empresa a un perfil de dispositivo.

Creación de un perfil de dispositivo

Antes de empezar: Para los dispositivos Samsung Knox, Crear avisos de la empresa.

1. En la barra de menús de la consola de administración, haga clic en **Políticas y perfiles > Personalizado > Dispositivo**.
2. Haga clic en +.
3. Escriba un nombre y una descripción para el perfil.
4. Lleve a cabo una de las tareas siguientes:

Tarea	Pasos
Asigne un aviso de la empresa para que se muestre en los dispositivos con Samsung Knox cuando un usuario reinicie su dispositivo.	En la pestaña **Android**, en la lista desplegable **Asignar aviso de la empresa**, seleccione el aviso de la empresa adecuado.
En los dispositivos iOS y Android, defina la información de la empresa que se mostrará en la aplicación de BlackBerry UEM Client. En Windows 10, defina el número de teléfono y la dirección de correo que se mostrarán en la información de soporte en los dispositivos.	En la pestaña del sistema operativo correspondiente, especifique el nombre, la dirección, el número de teléfono y la dirección de correo electrónico.

5. Opcionalmente, efectúe una de las acciones siguientes:

Tarea	Pasos
Adición de una imagen de fondo de pantalla al espacio de trabajo de los dispositivos con Samsung Knox.	**a.** En la pestaña **Android** , en la sección **Fondo de pantalla del espacio de trabajo**, haga clic en **Examinar**. **b.** Navegue a la imagen y selecciónela.
Adición de una imagen de fondo de pantalla a los dispositivos iOS supervisados.	En la pestaña **iOS**, en la sección **Fondo de pantalla del dispositivo**, efectúe una de las acciones siguientes: • Para establecer el fondo de pantalla de la pantalla de bloqueo, junto a **Imagen de la pantalla de bloqueo**, haga clic en **Examinar**. Navegue a la imagen y selecciónela. • Para establecer el fondo de pantalla de la pantalla de inicio, junto a **Imagen de la pantalla de inicio**, haga clic en **Examinar**. Navegue a la imagen y selecciónela.

6. Haga clic en **Agregar**.

Después de terminar:

- Asigne el perfil a usuarios y grupos.

- Si es necesario, clasifique el perfil.

Uso de servicios de ubicación en los dispositivos

Puede utilizar un perfil de servicio de ubicación para solicitar la ubicación de los dispositivos y ver las ubicaciones aproximadas en un mapa. También puede permitir que los usuarios localicen sus dispositivos mediante BlackBerry UEM Self-Service. Si activa el historial de ubicaciones para los dispositivos iOS y Android, los dispositivos deben aportar información sobre la ubicación de forma periódica y puede ver el historial de ubicaciones.

Los perfiles de los servicios de ubicación utilizan los servicios de ubicación en los dispositivos iOS, Android y Windows 10 Mobile. En función del dispositivo y de los servicios disponibles, es posible que los servicios de ubicación utilicen información de las redes móvil, GPS y Wi-Fi para determinar la ubicación del dispositivo.

Para activar y utilizar los servicios de ubicación, haga lo siguiente:

Paso	Acción
1	Configurar las opciones del servicio de ubicación.
2	Creación de un perfil de servicio de ubicación.
3	Ubicar un dispositivo.
4	De forma opcional, Activación del modo perdido para dispositivos iOS supervisados.

Configurar las opciones del servicio de ubicación

1. En la barra de menús de la consola de administración, haga clic en **Configuración > Configuración general > Servicios de ubicación**.
2. Si tiene un entorno local, en el campo **Antigüedad del historial de ubicación**, especifique cuánto tiempo desea que BlackBerry UEM almacene el historial de ubicación de los dispositivos. De forma predeterminada, UEM almacenará el historial durante un mes.
3. En la lista desplegable **Unidad de velocidad mostrada** haga clic en **km/h** o **mph**.
4. Haga clic en **Guardar**.

Después de terminar: Creación de un perfil de servicio de ubicación.

Creación de un perfil de servicio de ubicación

Antes de empezar: Configurar las opciones del servicio de ubicación.

1. En la barra de menús de la consola de administración, haga clic en **Políticas y perfiles > Protección > Servicios de ubicación**.
2. Haga clic en +.
3. Escriba un nombre y una descripción para el perfil.

4. Opcionalmente, desactive la casilla de verificación para cualquier tipo de dispositivo para el que no desee configurar el perfil.
5. Lleve a cabo cualquiera de las tareas siguientes:

Tarea	Pasos
Activar el historial de ubicaciones en dispositivos iOS	En la pestaña **iOS**, compruebe que la casilla de verificación **Registrar historial de ubicaciones de dispositivo** está seleccionada. BlackBerry UEM recopila la ubicación de un dispositivo cada hora y, si es posible, cuando haya un cambio significativo en la ubicación del dispositivo (por ejemplo, 500 metros o más).
Activar el historial de ubicaciones en dispositivos Android	**a.** En la pestaña **Android**, compruebe que la casilla de verificación **Registrar historial de ubicaciones de dispositivo** está seleccionada. **b.** En los campos **Distancia de comprobación de ubicación de dispositivo**, especifique la distancia mínima que un dispositivo debe recorrer antes de que se actualice la ubicación del dispositivo. **c.** En los campos **Frecuencia de actualización de la ubicación**, especifique con qué frecuencia se actualiza la ubicación del dispositivo. Se deben cumplir las condiciones de distancia y frecuencia antes de que se actualice la ubicación del dispositivo.

6. Haga clic en **Agregar**.

Después de terminar:

- Asigne el perfil a usuarios y grupos. Los usuarios deben aceptar el perfil con anterioridad para que la consola de gestión o BlackBerry UEM Self-Service muestren las ubicaciones de los dispositivos iOS y Android en un mapa. Los dispositivos Windows 10 Mobile aceptan automáticamente el perfil.
- Si es necesario, clasifique el perfil.
- Ubicar un dispositivo.

Ubicar un dispositivo

Antes de empezar: Creación de un perfil de servicio de ubicación.

1. En la barra de menús de la consola de administración, haga clic en **Usuarios > Dispositivos gestionados**.
2. Seleccione la casilla de verificación correspondiente a los dispositivos que desea ubicar.
3. Haga clic en .
4. Busque los dispositivos en el mapa mediante el icono de ubicación actual () y el icono de última ubicación conocida (). Si un dispositivo iOS o Android no responde con la última información de ubicación y el historial de ubicaciones está activado en el perfil, el mapa muestra la última ubicación conocida del dispositivo.
5. Haga clic o desplace el cursor sobre un icono para mostrar la información de ubicación, como la latitud y la longitud, y cuándo se informó de la ubicación.
6. Para ver el historial de ubicaciones de un dispositivo iOS o Android, haga clic en **Ver historial de ubicaciones**, seleccione un intervalo de fecha y hora y haga clic en **Enviar**.

Activación del modo perdido para dispositivos iOS supervisados

Puede activar y gestionar el modo perdido para dispositivos iOS supervisados. Cuando se pierde un dispositivo, puede activar el modo perdido para bloquearlo y configurar un mensaje para que se muestre, y puede ver la ubicación actual del dispositivo sin utilizar un perfil de servicio de ubicación.

1. En la barra de menús de la consola de administración, haga clic en **Usuarios > Dispositivos gestionados**.
2. Haga clic en un dispositivo.
3. En la pestaña del dispositivo, haga clic en **Activar modo perdido**.
4. En los campos **Número de teléfono de contacto** y **Mensaje**, escriba la información correspondiente.
5. De manera opcional, seleccione **Sustituir diapositiva para desbloquear texto** e introduzca el texto para mostrar.
6. Haga clic en **Activar**.

Después de terminar:

- Para localizar un dispositivo que está en el modo perdido, en la pestaña del dispositivo, haga clic en **Obtener ubicación del dispositivo**.
- Para desactivar el modo perdido, en la pestaña del dispositivo, haga clic en **Desactivar modo perdido**.

Habilitación del bloqueo de activación para un dispositivo iOS

La función de bloqueo de activación en dispositivos iOS permite a los usuarios proteger sus dispositivos si se pierden o se los roban. Cuando la función está activada, el usuario debe confirmar el ID y la contraseña de Apple ID para desactivar Buscar mi iPhone, borrar el dispositivo o reactivar y utilizar el dispositivo.

Cuando se activa un dispositivo en BlackBerry UEM, el bloqueo de activación está desactivado de forma predeterminada. Puede activarlo para cada dispositivo de forma individual o puede hacerlo para varios dispositivos utilizando la regla de política de TI asociada. Al activar el bloqueo de activación, UEM guarda un código de desvío que puede utilizar para borrar el bloqueo y que el dispositivo se pueda borrar y reactivar sin la contraseña ni el ID de Apple del usuario.

Complete los siguientes pasos para activar el bloqueo de activación para cada dispositivo de forma individual.

Antes de empezar:

- El dispositivo debe supervisarse.
- El dispositivo debe estar asociado a una cuenta iCloud.
- El dispositivo debe tener activada la opción Buscar mi iPhone o Buscar mi iPad.

1. En la consola de gestión de la barra de menú, haga clic en **Usuarios**.
2. Busque una cuenta de usuario y haga clic en ella.
3. En la pestaña del dispositivo, en la sección **Gestionar dispositivo**, haga clic en **Habilitar el bloqueo de activación**.

Después de terminar:

- Para desactivar el bloqueo de activación de un dispositivo, haga clic en **Desactivar bloqueo de activación**. Si se activa el bloqueo de activación utilizando la regla de política de TI, no podrá utilizar esta opción para desactivarlo.
- Para ver el código de omisión de un dispositivo, vaya a **Usuarios > Bloqueo de activación de Apple** y, a continuación, busque un dispositivo y haga clic en él.

Administración de las funciones de iOS mediante perfiles de carga personalizados

Se pueden utilizar perfiles de carga personalizados para controlar las funciones de los dispositivos iOS que no están controladas por las políticas o perfiles existentes de BlackBerry UEM. Si una función está controlada por una política o perfil existentes de UEM, un perfil de carga personalizado podría no funcionar según lo esperado. Debería utilizar las políticas o perfiles actuales, siempre que sea posible.

Puede crear perfiles de configuración de Apple mediante Apple Configurator y añadirlos a perfiles de carga personalizados de UEM. Se pueden asignar perfiles de carga personalizados a usuarios, grupos de usuarios y grupos de dispositivos.

Por ejemplo, desea controlar una nueva función que estará disponible para los dispositivos cuando se actualicen a una nueva versión de iOS, pero UEM no tendrá una regla de política de TI para esa nueva función hasta una futura versión del software de UEM. Para resolver este problema, puede crear un perfil de carga personalizado que controle esa función hasta que sea compatible de forma oficial con UEM.

Creación de un perfil de carga personalizado

Antes de empezar: Descargue e instale la última versión de Apple Configurator.

1. En Apple Configurator, cree un perfil de configuración de Apple.
2. Copie el código XML del perfil de configuración de Apple. Cuando copie el texto, copie únicamente los elementos en negrita como se muestra en el ejemplo de código siguiente.

```
<?xml version="1.0" encoding="UTF-8"?>
    <!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
    "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
    <plist version="1.0">
    <dict>
         <key>PayloadContent</key>
         <array>
               <dict>
                    <key>CalDAVAccountDescription</key>
                    <string>CalDAV Account Description</string>
                    <key>CalDAVHostName</key>
                    <string>caldav.server.example</string>
                    <key>CalDAVPort</key>
                    <integer>8443</integer>
                    <key>CalDAVPrincipalURL</key>
                    <string>Principal URL for the CalDAV account</string>
                    <key>CalDAVUseSSL</key>
                    </true>
                    <key>CalDAVUsername</key>
                    <string>Username</string>
                    <key>PayloadDescription</key>
                    <string>Configures CalDAV account.</string>
                    <key>PayloadDisplayName</key>
                    <string>CalDAV (CalDAV Account Description)</string>
                    <key>PayloadIdentifier</key>
                    <string>.caldav1</string>
                    <key>PayloadOrganization</key>
                    <string></string>
                    <key>PayloadType</key>
                    <string>com.apple.caldav.account</string>
```

```
                    <key>PayloadUUID</key>
                    <string>9ADCF5D6-397C-4E14-848D-FA04643610A3</string>
                    <key>PayloadVersion</key>
                    <integer>1</integer>
                </dict>
        </array>
        <key>PayloadDescription</key>
        <string>Profile description.</string>
        <key>PayloadDisplayName</key>
        <string>Profile Name</string>
        <key>PayloadOrganization</key>
        <string></string>
        <key>PayloadRemovalDisallowed</key>
        <false/>
        <key>PayloadType</key>
        <string>Configuration</string>
        <key>PayloadUUID</key>
        <string>7A5F8391-5A98-46EA-A3CF-C0D6EDC74632</string>
        <key>PayloadVersion</key>
        <integer>1</integer>
    </dict>
    </plist>
```

3. En la barra de menús de la consola de administración de UEM, haga clic en **Políticas y perfiles > Personalizado > Carga personalizada**.
4. Haga clic en +.
5. Escriba un nombre y una descripción para el perfil.
6. En el campo **Carga personalizada**, pegue el código XML que copió en el paso 2.
7. Haga clic en **Agregar**.

Después de terminar: Asigne el perfil a usuarios y grupos.

Gestión de la protección contra el restablecimiento de los datos de fábrica para dispositivos Android Enterprise y Android Management

Puede utilizar el perfil de protección contra el restablecimiento de los datos de fábrica para controlar la función de protección contra el restablecimiento de los datos de fábrica para los dispositivos Android Enterprise y Android Management de su empresa que se hayan activado mediante los tipos de activación Solo espacio de trabajo y Trabajo y personal: control total.

La protección contra el restablecimiento de los datos de fábrica requiere que un usuario del dispositivo Android introduzca sus credenciales de la cuenta de Google para desbloquear un dispositivo que se ha restablecido a la configuración de fábrica. Se activa de forma predeterminada cuando un usuario añade una cuenta de Google al dispositivo. Este perfil le permite desactivar la protección contra el restablecimiento de los datos de fábrica o especificar una cuenta de usuario que se puede utilizar para desbloquear un dispositivo después de que se haya restablecido a los datos de fábrica.

Los perfiles de protección contra el restablecimiento de los datos de fábrica ofrecen las siguientes opciones:

Opción	Descripción	Tipos de activación compatibles
Desactivar la protección contra el restablecimiento de los datos de fábrica	Cualquier persona puede restablecer la configuración de fábrica de un dispositivo perdido o robado y comenzar a utilizarlo. Esta opción es útil si un usuario conocido ha olvidado sus credenciales de la cuenta de Google o si le han devuelto un dispositivo que es propiedad de su empresa y necesita restablecerlo.	Android Enterprise
Activar y utilizar las credenciales de una cuenta de Google anterior al restablecer la configuración de fábrica de un dispositivo	Los usuarios pueden utilizar las credenciales de la cuenta de Google que ya están asociadas al dispositivo después de un restablecimiento de los datos de fábrica. Ésta es la configuración predeterminada. Si un dispositivo se restablece a la configuración de fábrica, el usuario debe iniciar sesión en el dispositivo utilizando las credenciales de la cuenta de Google que ya están en el dispositivo. Esto evita que alguien con un dispositivo perdido o robado pueda restablecerlo y utilizarlo.	Android Enterprise

Opción	Descripción	Tipos de activación compatibles
Habilitar y especificar las credenciales de la cuenta de Google cuando al restablecer el dispositivo a la configuración de fábrica	Puede especificar las credenciales de la cuenta de Google que un usuario puede utilizar para iniciar sesión en el dispositivo después de restablecer la configuración de fábrica. Esta opción permite a su empresa controlar quién puede iniciar sesión en un dispositivo después de restablecer la configuración de fábrica. Le recomendamos que utilice esta opción únicamente si conoce a fondo la experiencia del usuario del dispositivo. Si su empresa utiliza una cuenta administrada de Google Play, puede que desee utilizar esta opción porque no existe una cuenta de Google en los dispositivos de su empresa y, por lo tanto, la protección contra el restablecimiento de los datos de fábrica no está disponible en el dispositivo.	Android Enterprise Android Management

Existen varias formas en las que un dispositivo puede restablecer la configuración predeterminada de fábrica. La protección contra el restablecimiento de los datos de fábrica responde de forma diferente en función del método utilizado. Para obtener más información acerca del restablecimiento seguro y poco seguro, consulte KB 56972.

Creación de un perfil de protección contra el restablecimiento de los datos de fábrica

1. En la barra de menús de la consola de administración, haga clic en **Políticas y perfiles > Dispositivos gestionados > Protección > Protección contra el restablecimiento de los datos de fábrica**.
2. Haga clic en +.
3. Escriba un nombre y una descripción para el perfil.
4. En la lista desplegable **Configuración de protección contra el restablecimiento de los datos de fábrica**, haga clic en una de las siguientes opciones:
   - **Desactivar la protección contra el restablecimiento de los datos de fábrica**: si desactiva la protección contra el restablecimiento de los datos de fábrica, no se pedirá a los usuarios que introduzcan un ID de usuario de Google al restablecer la configuración de fábrica del dispositivo. Esta opción es compatible con dispositivos Android Enterprise (Trabajo y personal: control total y Solo espacio de trabajo).
   - **Activar y utilizar las credenciales de una cuenta de Google anterior cuando se restablezca la configuración de fábrica de un dispositivo**: esta es la opción predeterminada. Si el usuario restablece la configuración de fábrica del dispositivo utilizando un método que no es de confianza y ya había una cuenta de Google en el dispositivo antes del restablecimiento, la cuenta deberá verificarse después de restablecer el dispositivo a la configuración de fábrica. Tenga en cuenta que si su empresa utiliza estructura gestionada de cuentas de Google, la cuenta de Google dejará de existir en el dispositivo y la protección contra el restablecimiento de los datos de fábrica dejará de estar disponible en este. Esta opción es compatible con dispositivos Android Enterprise (Trabajo y personal: control total y Solo espacio de trabajo).
   - **Habilitar y especificar las credenciales de la cuenta de Google cuando se restablece el dispositivo a la configuración de fábrica**: seleccione esta opción para especificar la cuenta de Google que se debe utilizar para iniciar sesión en el dispositivo después de un restablecimiento de fábrica que no sea de confianza.

Si selecciona esta opción, no se pueden usar las credenciales de la cuenta de Google personal del usuario después del restablecimiento de fábrica. Esta opción es compatible con dispositivos Android Enterprise y Android Management (Trabajo y personal: control total y Solo espacio de trabajo).

Si desea utilizar una cuenta gestionada de Google Play, desactive la opción "Permitir restablecimiento de fábrica" en la política de TI asignada a los usuarios. Esto desactiva la opción de restablecimiento de fábrica en la configuración del dispositivo y el botón Desactivar en el UEM Client. Esto es para asegurarse de que los usuarios no utilicen la opción de desactivación no fiable en UEM Client que activa la protección contra el restablecimiento de los datos de fábrica en el dispositivo.

5. Si ha seleccionado **Habilitar y especificar las credenciales de la cuenta de Google cuando se restablece el dispositivo a la configuración de fábrica**, haga clic en + y realice una de las siguientes acciones para añadir cuentas de Google (puede añadir hasta 20):
   - Para utilizar la autenticación de Google, haga clic en **Añadir mediante la autenticación de Google** e inicie sesión en la cuenta de Google que desea utilizar para iniciar sesión en los dispositivos que se han restablecido.
   - Para especificar cuentas manualmente, haga clic en **Manual**. Especifique la dirección de correo electrónico y el ID de Google. Para obtener el ID de Google, haga lo siguiente en el sitio de la API de personas para desarrolladores de Google:
     a. En el campo **resourceName**, escriba: people/me.
     b. En el campo **personalFields**, escriba: metadata.
     c. Haga clic en **Ejecutar**.
     d. En la pantalla **Seleccionar una cuenta**, seleccione la cuenta que desea utilizar para configurar el perfil de protección contra el restablecimiento de los datos de fábrica.
     e. En la pantalla **El explorador de API de Google quiere acceder a su cuenta de Google**, haga clic en **Permitir**.
     f. En la página **People ID**, anote el ID de usuario de 21 dígitos.
6. Si ha seleccionado **Habilitar y especificar las credenciales de la cuenta de Google cuando se restablece el dispositivo a la configuración de fábrica** y su empresa tiene un dominio de Google Workspace o Google Cloud, seleccione **Añadir una cuenta de Google creada por BlackBerry UEM** si desea incluir la cuenta de Google de trabajo del usuario en la lista de cuentas que pueden desbloquear el dispositivo después de un restablecimiento de fábrica.
7. Haga clic en **Guardar**.

Después de terminar:

- Asigne el perfil a usuarios y grupos.
- Si es necesario, clasifique el perfil.
- Cuando se activa la protección contra el restablecimiento de los datos de fábrica en el dispositivo, la activación de la empresa en BlackBerry UEM no funciona. Primero, debe quitar la protección contra el restablecimiento de los datos de fábrica utilizando la configuración inicial de Android. Consulte Eliminación de la protección contra el restablecimiento de los datos de fábrica de un dispositivo.

Eliminación de la protección contra el restablecimiento de los datos de fábrica de un dispositivo

Cuando se activa la protección contra el restablecimiento de los datos de fábrica en el dispositivo, la activación de la empresa en BlackBerry UEM no funciona. Primero, debe quitar la protección contra el restablecimiento de los datos de fábrica utilizando la configuración inicial de Android.

1. Si utiliza cualquier tipo de sistema de activación automatizado (como el aprovisionamiento automático o Samsung Knox Mobile Enrollment), debe desactivarlo para que el dispositivo pueda volver a la configuración inicial.
2. Cuando el dispositivo tenga conectividad, en la primera pantalla de la cuenta de Android, se pedirá al usuario que introduzca las credenciales de la cuenta de Google asociadas al dispositivo. Si ha configurado una cuenta específica de Google en el perfil de protección contra el restablecimiento de los datos de fábrica, el usuario deberá introducir la dirección de correo y la contraseña asociadas a dicha cuenta.
3. Cuando el usuario haya introducido la dirección de correo electrónico y la contraseña de la cuenta de Google, se le preguntará si desea añadir el usuario al dispositivo. El usuario debe seleccionar la opción de utilizar un nuevo usuario para el dispositivo.
    - En los dispositivos que no sean Samsung y no utilicen el aprovisionamiento automático: los usuarios pueden introducir los datos de la cuenta de Google de la empresa para instalar BlackBerry UEM Client y volver a activar el dispositivo en UEM.
    - En los dispositivos Samsung que no utilizan el aprovisionamiento automático o Samsung Knox Mobile Enrollment: complete la configuración inicial y utilice la configuración del dispositivo para restablecerlo. Cuando el dispositivo se reinicie, podrá reactivarse.
    - Dispositivos con aprovisionamiento automático o Samsung Knox Mobile Enrollment: si utiliza cualquier tipo de sistema de activación automático (como el aprovisionamiento automático o Samsung Knox Mobile Enrollment), puede volver a activarlo para el dispositivo, completar la configuración inicial y utilizar la configuración del dispositivo para restablecerlo. Seguidamente, el dispositivo deberá reiniciarse y utilizar el sistema de activación automatizada que haya configurado.

Configuración de atestaciones de dispositivos

Al activar la atestación, BlackBerry UEM envía comprobaciones para probar la autenticidad y la integridad de los dispositivos. Puede activar la atestación para los dispositivos Samsung Knox, Android, iOS y Windows 10.

Configuración de atestaciones de dispositivos Android y aplicaciones de BlackBerry Dynamics

Puede utilizar SafetyNet o una atestación de Google Play Integrity para que BlackBerry UEM envíe comprobaciones para probar la autenticidad y la integridad de los dispositivos Android y las aplicaciones de BlackBerry Dynamics. SafetyNet y Play Integrity le permite evaluar la seguridad y la compatibilidad de los entornos en los que se ejecutan las aplicaciones de su empresa. Puede utilizar la atestación de SafetyNet o Play Integrity, además de la detección de utilización y origen existente de BlackBerry. Puede configurar y asignar un perfil de conformidad de UEM para llevar a cabo las acciones de conformidad adecuadas cuando los dispositivos o las aplicaciones fallen la atestación.

UEM utiliza la API de Play Integrity con versiones de UEM Client que la admiten para proporcionar protección adicional contra la manipulación de aplicaciones. Play Integrity reemplazará SafetyNet en función de la programación de migración determinada por Google. SafetyNet seguirá siendo compatible con versiones anteriores de UEM Client. Para obtener más información acerca de la migración desde SafetyNet, consulte Google Play: Migración desde la API de atestación de SafetyNet.

UEM realiza la atestación de SafetyNet o Play Integrity en las siguientes circunstancias:

- Tras la activación del dispositivo cuando BlackBerry UEM Client está instalado.
- Al activar las aplicaciones de BlackBerry Dynamics y después de hacerlo. Tenga en cuenta que UEM no confía en versiones anteriores de las aplicaciones. Para superar las comprobaciones de atestación, los dispositivos deben tener la última versión disponible de las aplicaciones de BlackBerry Dynamics.
- A petición mediante API de REST.
- Si el UEM Client está activado, cuando se reinicia un dispositivo.
- Comprobaciones de atestación periódicas con la frecuencia de comprobación que especifique.

No es necesario UEM Client para habilitar la atestación de SafetyNet o Play Integrity. El UEM Client no aparece en la lista de aplicaciones de BlackBerry Dynamics que puede configurar para la atestación de SafetyNet o Play Integrity, pero recibe las comprobaciones de atestación de UEM y responde a ellas.

Si el dispositivo de un usuario está fuera de cobertura, apagado o sin batería, no puede responder a las comprobaciones de atestación. En estas circunstancias, UEM considerará que el dispositivo no cumple los requisitos de conformidad y llevará a cabo las acciones que haya configurado en el perfil de conformidad asignado.

Configuración de atestaciones de dispositivos Android y aplicaciones de BlackBerry Dynamics

Antes de empezar: La última versión de los servicios de Google Play debe estar instalada en los dispositivos de los usuarios.

1. En la barra de menús de la consola de administración, haga clic en **Configuración > Configuración general > Atestación**.
2. Seleccione la casilla de verificación **Activar las comprobaciones de atestación con SafetyNet o Play Integrity**.
3. Si desea activar Google Compatibility Test Suite, seleccione la casilla de verificación **Activar la coincidencia de perfiles CTS**.

4. En la sección **Frecuencia de la comprobación**, especifique la frecuencia con la que el dispositivo debe devolver una respuesta de atestación a BlackBerry UEM. El valor predeterminado y mínimo es de 24 horas.
5. En la sección **Periodo de gracia**, especifique el periodo de gracia para los dispositivos. Cuando el periodo de gracia caduca sin una respuesta de atestación satisfactoria, un dispositivo se considera fuera de conformidad y está sujeto a las acciones que usted especifique en el perfil de conformidad asignado.
6. En la sección **Periodo de gracia de aplicación**, especifique un periodo de gracia para las aplicaciones BlackBerry Dynamics. Cuando el periodo de gracia caduca sin una respuesta de atestación satisfactoria, una aplicación de BlackBerry Dynamics está sujeta a las acciones que usted especifique en el perfil de conformidad asignado. El periodo de gracia se aplica según la aplicación.
7. Para especificar las aplicaciones de BlackBerry Dynamics que estarán sujetas a las comprobaciones de atestación, haga clic en +.
8. Seleccione las aplicaciones y haga clic en **Seleccionar**.
9. Haga clic en **Guardar**.

Después de terminar:

- En el perfil de conformidad asignado a los dispositivos, active la regla "error de atestación de SafetyNet o Play Integrity" y configure las acciones que desea que UEM lleve a cabo cuando los dispositivos o las aplicaciones de BlackBerry Dynamics no cumplan la atestación.
- En la consola de administración, puede ver el estado de atestación de un dispositivo en los detalles del dispositivo.

Configuración de atestaciones de dispositivos iOS

Cuando habilita la atestación para los dispositivos iOS, se garantiza que solo se utilicen dispositivos autorizados y no comprometidos en su organización. Durante la atestación, se verifica que las propiedades del dispositivo (por ejemplo, su número de serie) o los identificadores son legítimos y no han sido falsificados. Esta función requiere que los dispositivos no supervisados ejecuten iOS 16 o iPadOS 16.1, o versiones posteriores. Para los dispositivos supervisados, se requiere iOS 17 o iPadOS se 17, o versiones posteriores.

1. En la barra de menús de la consola de administración, haga clic en **Configuración > Configuración general > Atestación**.
2. Seleccione la casilla de verificación **Activar las comprobaciones de atestación periódicas para los dispositivos Apple que ejecuten iOS 16 o posterior**.
3. En la sección **Frecuencia de la comprobación**, especifique la frecuencia con la que el dispositivo debe devolver una respuesta de atestación a UEM. La frecuencia de comprobación mínima es de 9 días.
4. En la sección **Periodo de gracia**, especifique el periodo de gracia para los dispositivos. Cuando el periodo de gracia caduca sin una respuesta de atestación satisfactoria, un dispositivo se considera fuera de conformidad y está sujeto a las acciones que usted especifique en el perfil de conformidad asignado.
5. Haga clic en **Guardar**.

Después de terminar:

- En el perfil de activación, especifique si la atestación se produce durante la activación del dispositivo o periódicamente. La atestación de dispositivos gestionados se aplica a los tipos de activación Controles de MDM y Privacidad del usuario, pero no al tipo de activación Privacidad de usuario: inscripción de usuario. Cuando selecciona el tipo de activación Privacidad del usuario en el perfil de activación, debe seleccionar al menos una de las opciones de administración (como "Permitir administración de VPN").
- En el perfil de conformidad, seleccione la regla "Fallo de atestación de dispositivos gestionados" y especifique las acciones de conformidad que desea que se lleven a cabo en los dispositivos en los que falle la atestación.
- En la consola de administración, puede ver el estado de atestación de un dispositivo en los detalles del dispositivo.

Configuración de atestaciones de dispositivos Samsung Knox

Si activa la atestación, BlackBerry UEM envía comprobaciones para probar la autenticidad y la integridad de los dispositivos Samsung Knox con los siguientes tipos de activación:

- Trabajo y personal: control total (Samsung Knox)
- Trabajo y personal: privacidad de usuario (Samsung Knox)

1. En la barra de menús de la consola de administración, haga clic en **Configuración > Configuración general > Atestación**.
2. Seleccione la casilla de verificación **Activar las comprobaciones de atestación periódicas para los dispositivos con KNOX Workspace**.
3. En la sección **Frecuencia de la comprobación**, especifique la frecuencia con la que el dispositivo debe devolver una respuesta de atestación a UEM.
4. En la sección **Periodo de gracia**, especifique el periodo de gracia para los dispositivos. Cuando el periodo de gracia caduca sin una respuesta de atestación satisfactoria, un dispositivo se considera fuera de conformidad y está sujeto a las acciones que usted especifique en el perfil de conformidad asignado.
5. Haga clic en **Guardar**.

Después de terminar: En el perfil de conformidad asignado a los dispositivos, active la regla "Atestación con errores de Knox o con rooting de SO" y configure las acciones que desea que UEM lleve a cabo cuando los dispositivos fallen la atestación.

Configuración de atestaciones de dispositivos Windows 10

Al activar la atestación, BlackBerry UEM envía comprobaciones para probar la autenticidad y la integridad de los dispositivos Windows 10. Tenga en cuenta que la configuración de atestación de Windows 10 no se aplica a BlackBerry Desktop (BlackBerry Access + BlackBerry Work).

1. En la barra de menús de la consola de administración, haga clic en **Configuración > Configuración general > Atestación**.
2. Seleccione la casilla de verificación **Activar las comprobaciones de atestación periódicas para los dispositivos Windows 10**.
3. En la sección **Frecuencia de la comprobación**, especifique la frecuencia con la que el dispositivo debe devolver una respuesta de atestación a UEM.
4. En la sección **Periodo de gracia**, especifique el periodo de gracia para los dispositivos. Cuando el periodo de gracia caduca sin una respuesta de atestación satisfactoria, un dispositivo se considera fuera de conformidad y está sujeto a las acciones que usted especifique en el perfil de conformidad asignado.
5. Haga clic en **Guardar**.

Después de terminar: Cree un perfil de cumplimiento que especifique las acciones que se producen cuando se considera que un dispositivo tiene acceso a la raíz. Para obtener instrucciones, consulte Cumplimiento de las reglas de los dispositivos

Después de terminar:

- En el perfil de conformidad asignado a los dispositivos, configure las reglas de atestación del estado del dispositivo Windows y las acciones que desea que UEM lleve a cabo cuando los dispositivos fallen la atestación.
- En la consola de administración, puede ver el estado de atestación de un dispositivo en los detalles del dispositivo.

Configuración de Windows Information Protection de para dispositivos Windows 10

Puede configurar Windows Information Protection (WIP) para dispositivos Windows 10 cuando desee:

- Separar los datos personales de los de trabajo en los dispositivos.
- Borrar solo los datos de trabajo de los dispositivos.
- Evitar que los usuarios compartan los datos de trabajo fuera de aplicaciones de trabajo protegidas o con personas que no forman parte de su empresa.
- Proteger los datos incluso si se mueven o se comparten en otros dispositivos, como una llave USB.
- Auditar el comportamiento de los usuarios y tomar las medidas correspondientes para evitar pérdidas de datos.

Al configurar WIP para los dispositivos, puede especificar las aplicaciones que desea proteger. Las aplicaciones protegidas son de confianza para crear y acceder a los archivos de trabajo, mientras que a las aplicaciones sin protección se les puede bloquear el acceso a los archivos de trabajo. Puede elegir el nivel de protección para aplicaciones protegidas en función de cómo desea que los usuarios se comporten al compartir los datos de trabajo. Cuando está activada la WIP, todas las prácticas de intercambio se auditan. Las aplicaciones que especifique pueden habilitarse o inhabilitarse para la empresa. Las aplicaciones habilitadas pueden crear y acceder a los datos personales y de trabajo. Las aplicaciones inhabilitadas solo pueden crear y acceder a los datos de trabajo.

1. En la barra de menús de la consola de administración, haga clic en **Políticas y perfiles > Protección > Windows Information Protection**.
2. Haga clic en +.
3. Escriba un nombre y una descripción para el perfil.
4. Configure los valores adecuados para la configuración de cada perfil. Consulte Configuración del perfil de Windows Information Protection.
5. Haga clic en **Agregar**.

Después de terminar:

- Asigne el perfil a usuarios y grupos.
- Si es necesario, clasifique el perfil.

Configuración del perfil de Windows Information Protection

Configuración de perfil	Descripción
Configuración de Windows Information Protection	Esta configuración especifica si se ha activado Windows Information Protection y el nivel de aplicación. • Desactivación: los datos no se cifran y el registro de auditoría se desactiva. • Silencio: los datos se cifran y se registra cualquier intento de compartir datos protegidos. • Anulación: los datos se cifran, se avisa al usuario cuando intenta compartir datos protegidos y se registra cualquier intento de compartir datos protegidos. • Bloqueo: los datos se cifran, los usuarios no pueden compartir datos protegidos y se registra cualquier intento de compartir datos protegidos.

Configuración de perfil	Descripción
Nombres de dominio protegidos de la empresa	Esta configuración especifica los nombres de dominio de la red de trabajo que utiliza su empresa para las identidades de usuario. Separar varios dominios con barras (|). El primer dominio se utiliza como cadena para etiquetar los archivos que están protegidos por aplicaciones que utilizan WIP (por ejemplo, ejemplo.com|ejemplo.net).
Archivo de certificado de recuperación de datos (.der, .cer)	Esta configuración especifica el archivo del certificado de recuperación de datos que se utiliza para recuperar archivos protegidos localmente en un dispositivo. El archivo debe ser un certificado codificado PEM o DER con una extensión .der o .cer.
Eliminar la configuración de Windows Information Protection cuando se elimine un dispositivo de BlackBerry UEM	Esta configuración especifica si se revoca la configuración WIP cuando se desactiva un dispositivo. Cuando se revoca la configuración de WIP, el usuario ya no puede acceder a los archivos protegidos.
Mostrar superposiciones de Windows Information Protection en aplicaciones y archivos protegidos que pueden crear contenidos de la empresa	Esta configuración especifica si se muestra un icono superpuesto en los archivos y los iconos de aplicaciones para indicar si un archivo o aplicación está protegido por WIP.
Rango IP de la red de trabajo	Esta configuración especifica el intervalo de direcciones IP en el trabajo con las que puede compartir datos una aplicación protegida con WIP. Utilice un guión para indicar un rango de direcciones. Utilice una coma para separar las direcciones.
Los intervalos de IP de red de trabajo son autoritativos	Esta configuración especifica si solo se aceptan los intervalos IP de la red de trabajo como parte de la red de trabajo. Cuando se activa esta opción, no se realizan intentos para descubrir otras redes de trabajo.
Servidores de proxy internos de la empresa	Esta configuración especifica los servidores proxy internos que se utilizan cuando se conecta a ubicaciones de la red de trabajo. Estos servidores proxy solo se utilizan al conectarse al dominio indicado en la configuración de recursos de la nube de la empresa.
Recursos en la nube de la empresa	En la configuración se especifica la lista de dominios de recursos de empresa alojados en la nube que se deben proteger. Los datos de estos recursos se consideran los datos de la empresa y se protegen.
Dominio de recursos en la nube	En la configuración se especifica el nombre de dominio.

Configuración de perfil	Descripción
Proxy emparejado	En la configuración se especifica un proxy que está emparejado con un recurso en la nube. El tráfico al recurso de nube se enrutará a través de la red empresarial mediante el servidor proxy denotado (en el puerto 80). También se debe configurar un servidor proxy para este propósito en el campo Servidores de proxy internos de la empresa.
Servidores proxy de la empresa	Esta configuración especifica la lista de servidores proxy de internet.
Los servidores proxy de la empresa son autoritativos	Esta configuración especifica si el cliente debe aceptar la lista configurada de servidores proxy y no intentar detectar otros proxy de empresa.
Recursos neutrales	En la configuración se especifican los dominios que desea que se puedan utilizar para recursos de trabajo o personales.
Nombres de dominio de la red de la empresa	Esta configuración especifica una lista de dominios separada por comas que abarca los límites de la empresa. Los datos procedentes de uno de dichos dominios que se envíen a un dispositivo se considerarán datos de la empresa y estarán protegidos. Estas ubicaciones se considerarán destinos seguros para compartir los datos de la empresa.

Código de carga de las aplicaciones de escritorio	Especifique las claves de las aplicaciones de escritorio y los valores utilizados para configurar las restricciones de inicio de las aplicaciones en los dispositivos con Windows 10. Debe utilizar las claves definidas por Microsoft para el tipo de carga que desea configurar.
	Para especificar las aplicaciones, copie el código XML del archivo .xml de la política AppLocker y péguelo en este campo. Cuando copie el texto, copie únicamente los elementos como se muestran en el ejemplo de código siguiente.
	`<RuleCollection Type="Appx" EnforcementMode="Enabled">`
	`  <FilePublisherRule Id="0c9781aa-bf9f-4352-`
	`b4ba-64c25f36f558"`
	`  Name="WordMobile" Description="`
	` UserOrGroupSid="S-1-1-0" Action="Allow">`
	`  <Conditions>`
	`  <FilePublisherCondition`
	`  PublisherName="CN=Microsoft Corporation, O=Microsoft`
	` Corporation, L=Redmond, S=Washington, C=US"`
	`  ProductName="Microsoft.Office.Word" BinaryName="*">`
	`  <BinaryVersionRange LowSection="*"`
	` HighSection="*" />`
	`  </FilePublisherCondition>`
	`  </Conditions>`
	`  </FilePublisherRule>`
	`</RuleCollection>`

Configuración de perfil	Descripción

Código de carga de las aplicaciones de Universal Windows Platform	Especifique las claves y los valores de las aplicaciones de Universal Windows Platform utilizados para configurar WIP en dispositivos con Windows 10. Debe utilizar las claves definidas por Microsoft para el tipo de carga que desea configurar.
	
	Para especificar las aplicaciones, copie el código XML del archivo .xml de la política AppLocker y péguelo en este campo. Cuando copie el texto, copie únicamente los elementos como se muestran en el ejemplo de código siguiente.
	
	`<RuleCollection Type="Exe" EnforcementMode="Enabled">`
	`  <FilePathRule Id="921cc481-6e17-4653-8f75-050b80acca20"`
	`  Name="(Default Rule)`
	`  All files" Description="" UserOrGroupSid="S-1-1-0"`
	`  Action="Allow">`
	`  <Conditions>`
	`  <FilePathCondition Path="*" />`
	`  </Conditions>`
	`  </FilePathRule>`
	`  <FilePublisherRule Id="ddd0bc90-`
	`dada-4002-9e2f-0fc68e1f6af0" Name="WORDPAD.EXE,`
	`  from O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON,`
	`  C=US" Description=""`
	`  UserOrGroupSid="S-1-1-0" Action="Deny">`
	`  <Conditions>`
	`  <FilePublisherCondition PublisherName="O=MICROSOFT`
	`  CORPORATION`
	`  L=REDMOND, S=WASHINGTON, C=US" ProductName="*"`
	`  BinaryName="WORDPAD.EXE">`
	`  <BinaryVersionRange LowSection="*"`
	`  HighSection="*" />`
	`  </FilePublisherCondition>`
	`  </Conditions>`
	`  </FilePublisherRule>`
	`  <FilePublisherRule Id="c8360d06-f651-4883-`
	`abdd-9c3a95a415ff" Name="NOTEPAD.EXE,`
	`  from O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON,`
	`  C=US" Description=""`
	`  UserOrGroupSid="S-1-1-0" Action="Allow">`
	`  <Conditions>`
	`  <FilePublisherCondition PublisherName="O=MICROSOFT`
	`  CORPORATION,`
	`  L=REDMOND, S=WASHINGTON, C=US" ProductName="*"`
	`  BinaryName="NOTEPAD.EXE">`
	`  <BinaryVersionRange LowSection="*"`
	`  HighSection="*" />`
	`  </FilePublisherCondition>`
	`  </Conditions>`
	`  </FilePublisherRule>`
	`</RuleCollection>`

Perfil VPN asociado	Esta configuración especifica el perfil VPN que un dispositivo utiliza para conectarse a una red VPN cuando utiliza una aplicación protegida por WIP. Esta configuración solo es válida si está seleccionado "Utilizar un perfil de VPN" para "Conexión segura utilizada con WIP".

Configuración de perfil	Descripción
Recopilar registros de auditoría del dispositivo	En la configuración se especifica si desea recopilar registros de auditoría del dispositivo.

Movimiento de dispositivos con iOS o macOS a un canal reforzado

Cuando se activan dispositivos con iOS o macOS, de forma predeterminada se asignan a un canal de datos reforzado. Si tiene algún dispositivo con iOS o macOS que actualmente no utilice un canal reforzado, puede exportar una lista con esos dispositivos y tomar medidas para moverlos a un canal reforzado. Al mover dispositivos a un canal reforzado, deben volver a activarse.

Si mueve un dispositivo inscrito en DEP de Apple, el dispositivo perderá la configuración de inscripción de DEP. Los usuarios del dispositivo tendrán que restablecer la configuración de fábrica del dispositivo y activarlo de nuevo con BlackBerry UEM.

Antes de empezar: En la configuración de la aplicación de todas las aplicaciones relevantes, desactive la opción **Eliminar la aplicación del dispositivo cuando este se haya eliminado de BlackBerry UEM**. Si intenta mover dispositivos a un canal reforzado sin desactivar esta opción, la aplicación se eliminará y el dispositivo podría desinscribirse de UEM. Tenga en cuenta que, aunque desmarque esta casilla de verificación, es posible que una aplicación se elimine durante el traslado si la configuración no se ha entregado al dispositivo. Para obtener más información acerca de los comandos de seguimiento que se entregan a un dispositivo, consulte KB 102688.

1. En la barra de menús de la consola de administración, haga clic en **Configuración > Migración > Canal protegido de iOS** o **Configuración > Migración > Canal protegido de macOS**.

   Si no ve una de estas opciones de menú, su entorno UEM no tiene ningún dispositivo con iOS o macOS que deba moverse a un canal reforzado.
2. Haga clic en **Exportar** para descargar una lista de los dispositivos que actualmente no utilizan un canal reforzado.
3. Efectúe una de las acciones siguientes:

Tarea	Pasos
Mueva varios dispositivos con iOS a un canal reforzado.	Haga clic en **Examinar**, desplácese hasta el archivo que descargó en el paso 2 y selecciónelo. Los dispositivos que pertenecen a grupos de dispositivos compartidos se incluyen en el archivo únicamente con fines informativos y no se moverán a un canal reforzado con este método. Para cualquier dispositivo que pertenezca a grupos de dispositivos compartidos, el usuario debe restablecer la configuración de fábrica del dispositivo y activarlo de nuevo con UEM. Este método puede procesar un máximo de 1000 entradas a la vez. Si el archivo que ha descargado contiene más de 1000 entradas, divídalo en archivos separados que contengan un máximo de 1000 entradas cada uno.
Mueva un dispositivo iOS específico a un canal reforzado.	**a.** En la barra de menús, haga clic en **Usuarios > Dispositivos gestionados**. **b.** Busque el dispositivo con iOS y haga clic en él. **c.** En la pestaña de dispositivos, haga clic en **Migrar a canal reforzado iOS**. **d.** Haga clic en **Submit**.

Tarea	Pasos
Mueva los dispositivos macOS a un canal reforzado.	Póngase en contacto con los usuarios del dispositivo e indíqueles que reactiven el dispositivo con UEM Self-Service.

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