BlackBerry UEM

Gestión de las funciones del dispositivo

Administración

12.17

Contents

Gestión de las funciones y el comportamiento del dispositivo.....6

Gestión de dispositivos con políticas de TI.....7
Restricción o autorización de las capacidades del dispositivo.....7
Establecimiento de los requisitos de la contraseña del dispositivo.....8
Establecimiento de los requisitos de la contraseña de iOS.....8
Establecimiento de los requisitos de la contraseña de macOS.....9
Establecimiento de los requisitos de la contraseña de Android.....10
Establecimiento de los requisitos de la contraseña de Windows 10.....19
Creación y gestión de políticas de TI.....20
Creación de una política de TI.....20
Copie una política de TI.....20
Clasificar políticas de TI.....21
Presentación de políticas de TI.....21
Cambiar una política de TI.....21
Eliminación de una política de TI de las cuentas o de los grupos de usuarios.....21
Eliminar una política de TI.....22
Exporte las políticas de TI.....22
¿Cómo elige BlackBerry UEM qué política de TI asignar?.....23

Importación de las políticas de TI y las actualizaciones de metadatos del dispositivo.....24
Importación de las políticas de TI y las actualizaciones de metadatos del dispositivo manualmente.....24

Creación de mensajes de ayuda del dispositivo.....25
Crear mensajes de ayuda del dispositivo.....25

Cumplimiento de las reglas de los dispositivos.....26
Creación de un perfil de conformidad.....26
Configuración del perfil de conformidad.....27
Común: configuración del perfil de conformidad.....27
iOS: configuración del perfil de conformidad.....31
macOS: configuración del perfil de conformidad.....34
Android: Configuración del perfil de conformidad.....35
Windows: Configuración del perfil de conformidad.....39
Gestión de perfiles de conformidad de BlackBerry Dynamics.....42

Envío de comandos para los usuarios y dispositivos.....44
Enviar un comando a un dispositivo.....44
Envío de un comando masivo.....44
Establecer un tiempo de caducidad para comandos.....46

Referencia de comandos....46
Comandos para dispositivos con iOS....46
Comandos para dispositivos con macOS....49
Comandos para dispositivos Android....50
Comandos para dispositivos con Windows....53

Desactivación de dispositivos....56

Control de las actualizaciones de software instaladas en los dispositivos....57
Crear un perfil de requisitos de solicitud de servicio del dispositivo para dispositivos con Android Enterprise....58
Crear un perfil de requisitos de solicitud de servicio del dispositivo para dispositivos con Samsung Knox....59
Añadir una licencia de E-FOTA....60
Presentación de los usuarios que están ejecutando una versión de software rechazada....61
Gestión de actualizaciones del sistema operativo en dispositivos con activaciones de Controles de MDM....61
Vea las actualizaciones disponibles para dispositivos iOS....62
Actualización del SO en dispositivos de iOS supervisados....62

Configuración de la comunicación entre los dispositivos y BlackBerry UEM....63
Creación de un perfil de Enterprise Management Agent....63
iOS: configuración del perfil de Enterprise Management Agent....63
Android: configuración del perfil de Enterprise Management Agent....64
Windows: configuración del perfil de Enterprise Management Agent....65

Presentación de la información de la empresa en los dispositivos....66
Crear avisos de la empresa....67
Creación de un perfil de dispositivo....67

Uso de servicios de ubicación en los dispositivos....69
Configurar las opciones del servicio de ubicación....69
Creación de un perfil de servicio de ubicación....69
Ubicar un dispositivo....70
Uso del modo perdido para dispositivos iOS supervisados....71
Activar modo perdido....71
Localización de un dispositivo en modo perdido....71
Desactivar modo perdido....71

Bloqueo de activación en los dispositivos iOS....72
Activar bloqueo de activación....72
Desactivar bloqueo de activación....72
Visualice el código de desvío del bloqueo de activación....73

Administración de las características de iOS mediante perfiles de carga personalizados....74
Creación de un perfil de carga personalizado....74

Gestión de la protección contra el restablecimiento de los datos de fábrica para dispositivos Android Enterprise..... 76
Creación de un perfil de protección contra el restablecimiento de los datos de fábrica..... 76
Obtención manual de un ID de usuario para una cuenta de Google..... 77
¿Cómo responde la protección contra el restablecimiento de los datos de fábrica ante los restablecimiento del dispositivo?..... 77
Consideraciones para el uso de una cuenta de Google Play gestionada específica cuando se configura un perfil de protección contra el restablecimiento de los datos de fábrica..... 78
Eliminación de la protección contra el restablecimiento de los datos de fábrica de un dispositivo..... 79

Configuración de Windows Information Protection para dispositivos con Windows 10..... 80
Creación de un perfil de Windows Information Protection..... 80
Windows 10: configuración de perfil de Windows Information Protection..... 81

Activación del cifrado BitLocker en dispositivos con Windows 10..... 86

Administración de atestación para dispositivos..... 87
Administración de los dispositivos con Samsung Knox..... 87
Gestión de atestaciones de dispositivos Android y aplicaciones de BlackBerry Dynamics mediante SafetyNet..... 87
Consideraciones para configurar la atestación de SafetyNet 88
Configuración de atestaciones de dispositivos Android y aplicaciones de BlackBerry Dynamics mediante SafetyNet..... 89
Administración de los dispositivos con Windows 10..... 90

Migre dispositivos iOS para utilizar un canal protegido..... 91
Migrar un dispositivo iOS para utilizar un canal protegido..... 91
Exportar una lista de dispositivos macOS que requieran reactivación para utilizar un canal protegido..... 91

Aviso legal..... 92

Gestión de las funciones y el comportamiento del dispositivo

Tiene varias opciones para controlar el comportamiento del dispositivo. Puede utilizar los perfiles y las políticas de TI para activar o limitar el uso de varias funciones. También puede enviar comandos a los dispositivos para iniciar varias acciones.

Puede especificar la configuración de los diferentes tipos de dispositivos en la misma política de TI o el mismo perfil y, a continuación, asignar la política de TI o el perfil a las cuentas de usuario, a los grupos de usuarios o a los grupos de dispositivos.

Gestión de dispositivos con políticas de TI

Puede utilizar las políticas de TI para gestionar la seguridad y el comportamiento de los dispositivos en su empresa. Una política de TI es un conjunto de reglas que controla las características y la funcionalidad de los dispositivos. Puede configurar las reglas de todos los tipos de dispositivos en la misma política de TI. El SO del dispositivo determina la lista de características que se pueden controlar mediante políticas de TI y el tipo de activación del dispositivo determina qué reglas de una política de TI se aplican a un dispositivo concreto. Los dispositivos ignoran las reglas de la política de TI que no se les aplican.

BlackBerry UEM incluye una política de TI predeterminada con reglas preconfiguradas para cada tipo de dispositivo. 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, BlackBerry UEM envía la política de TI predeterminada a los dispositivos del usuario. BlackBerry 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.

BlackBerry UEM local se sincroniza diariamente con BlackBerry Infrastructure a través del puerto 3101 para determinar si hay disponible información actualizada de política de TI. Si hay información de la política de TI actualizada disponible, BlackBerry UEM la recupera y, de forma predeterminada, guarda las actualizaciones en la base de datos de BlackBerry UEM. A los administradores con los permisos "Ver políticas de TI" y "Crear y editar políticas de TI" se les notifica acerca de la actualización cuando inician sesión. Si la política de seguridad de su empresa no permitiera actualizaciones automáticas, puede desactivarlas e importar actualizaciones en BlackBerry UEM de forma manual. Para obtener más información, consulte Importación de las políticas de TI y las actualizaciones de metadatos del dispositivo.

La información de políticas de TI actualizada se aplica automáticamente en instancias de UEM Cloud.

Para obtener más información acerca de las reglas de políticas de TI para cada tipo de dispositivo, descargue la hoja de cálculo de referencia de políticas.

Restricción o autorización de las capacidades del dispositivo

Al configurar las reglas de políticas de TI, puede restringir o permitir las capacidades del dispositivo. Las reglas de políticas de TI disponibles para cada tipo de dispositivo están determinadas por el sistema operativo del dispositivo y por su versión, y por el tipo de activación del dispositivo. Por ejemplo, dependiendo del tipo de dispositivo y de activación, puede utilizar reglas de políticas de TI para:

- Imponer requisitos de contraseña para el dispositivo o el espacio de trabajo en un dispositivo
- Impedir que los usuarios utilicen funciones del dispositivo, como la cámara
- Controlar conexiones que utilizan la tecnología inalámbrica Bluetooth
- Controlar la disponibilidad de algunas aplicaciones
- Requerir cifrado y otras características de seguridad

Dependiendo del tipo de activación del dispositivo, puede utilizar las reglas de política de TI para controlar todo el dispositivo, solo el espacio de trabajo en un dispositivo, o ambos.

En los dispositivos con Android 8.0 y versiones posteriores, puede crear un mensaje de ayuda del dispositivo que se muestra en el dispositivo cuando algunas funciones cuando se desactivan debido a reglas de políticas de TI.

Para obtener más información acerca de las reglas de políticas de TI para cada tipo de dispositivo, descargue la hoja de cálculo de referencia de políticas.

Establecimiento de los requisitos de la contraseña del dispositivo

Puede utilizar las reglas de políticas de TI para configurar los requisitos de la contraseña de los dispositivos. Puede configurar los requisitos sobre la longitud y la complejidad de la contraseña, la caducidad de esta y el resultado del seguimiento de contraseñas incorrectas. Los temas siguientes explican las reglas de las contraseñas que se aplican a los distintos dispositivos y a los tipos de activación.

Para obtener más información acerca de las reglas de políticas de TI, descargue la hoja de cálculo de referencia de políticas.

Establecimiento de los requisitos de la contraseña de iOS

Puede elegir si los dispositivos iOS y iPadOS deben tener una contraseña. Si se requiere una contraseña, puede establecer los requisitos para esta.

Nota: Los dispositivos iOS y iPadOS y algunas reglas para la contraseña del dispositivo utilizan el término "código de acceso". Ambos, tanto "contraseña" como "código de acceso", tienen el mismo significado.

Regla	Descripción
Se requiere contraseña para el dispositivo	Especifique si el usuario debe establecer una contraseña para el dispositivo.
Permitir valor simple	Especifique si la contraseña puede contener caracteres repetidos o secuenciales, como DEFG o 3333.
Requerir valor alfanumérico	Especifique si la contraseña deberá contener letras y números.
Longitud mínima del código	Especifique la longitud mínima de la contraseña. Si introduce un valor que es menor que el mínimo requerido por el dispositivo, se utiliza dicho mínimo.
Número mínimo de caracteres complejos	Especifique el número mínimo de caracteres no alfanuméricos que debe contener la contraseña del dispositivo.
Periodo máximo de validez del código	Especifique el número máximo de días que puede utilizarse la contraseña.
Bloqueo automático máximo	Especifique el valor máximo que un usuario puede establecer para el tiempo de bloqueo automático, que se corresponde con el número de minutos de inactividad del usuario que deben transcurrir antes de que el dispositivo se bloquee. Si se establece en "Ninguno", todos los valores compatibles estarán disponibles en el dispositivo. Si el valor seleccionado se encuentra fuera del intervalo compatible con el dispositivo, el dispositivo utilizará el valor más cercano compatible.
Historial de códigos	Especifique el número de contraseñas anteriores que el dispositivo debe comprobar para evitar que un usuario vuelva a utilizar una contraseña reciente.

Regla	Descripción
Periodo máximo de gracia para el bloqueo del dispositivo	Especifique el valor máximo que un usuario puede establecer para el periodo de gracia para el bloqueo del dispositivo, que se corresponde con la cantidad de tiempo que un dispositivo puede permanecer bloqueado antes de que se requiera una contraseña para desbloquearlo. Si se establece en "Ninguno", todos los valores estarán disponibles en el dispositivo. Si se establece en "Inmediatamente", la contraseña se necesita inmediatamente después de que el dispositivo se bloquee.
Número máximo de intentos de contraseña fallidos	Especifique el número de veces que un usuario puede introducir una contraseña incorrecta antes de que se eliminen los datos del dispositivo.
Permitir cambios de contraseñas (solo con supervisión)	Especifique si un usuario puede agregar, cambiar o eliminar la contraseña.

Para obtener más información acerca de las reglas de contraseñas de las políticas de TI, descargue la hoja de cálculo de referencia de políticas.

Establecimiento de los requisitos de la contraseña de macOS

Puede elegir si las reglas de contraseña para dispositivos con macOS se aplican al dispositivo o al usuario y si es necesaria una contraseña. Si se requiere una contraseña, puede establecer los requisitos para esta.

Regla	Descripción
Objetivo de las reglas de políticas de TI	Esta regla especifica si las reglas de políticas de TI para la contraseña deben aplicarse únicamente a la cuenta del usuario asignado o a la totalidad del dispositivo.
Se requiere contraseña para el dispositivo	Especifique si el usuario debe establecer una contraseña para el dispositivo.
Permitir contraseña sencilla	Especifique si la contraseña puede contener caracteres repetidos o secuenciales, como DEFG o 3333.
Requerir valor alfanumérico	Especifique si la contraseña deberá contener letras y números.
Longitud mínima de la contraseña:	Especifique la longitud mínima de la contraseña.
Número mínimo de caracteres complejos	Especifique el número mínimo de caracteres no alfanuméricos que debe contener la contraseña del dispositivo.
Tiempo máximo de validez de la contraseña	Especifique un número de días máximo durante el cual se pueda utilizar la contraseña antes de caducar y que el usuario deba establecer una contraseña nueva.

Regla	Descripción
Bloqueo automático máximo	Especifique el número máximo de minutos de inactividad del usuario que debe transcurrir antes de que un dispositivo se bloquee. Si se ha configurado en "Ninguno", el usuario puede seleccionar cualquier valor.
Historial de contraseñas	Especifique el número máximo de contraseñas anteriores que el dispositivo debe comprobar para evitar que un usuario vuelva a utilizar una contraseña.
Periodo máximo de gracia para el bloqueo del dispositivo	Especifique el valor máximo que un usuario puede establecer para el periodo de gracia para el bloqueo del dispositivo, que se corresponde con la cantidad de tiempo que un dispositivo puede permanecer bloqueado antes de que se requiera una contraseña para desbloquearlo.
Número máximo de intentos de contraseña fallidos	Especifique el número de veces que un usuario puede introducir una contraseña incorrecta antes de que se eliminen los datos del dispositivo.

Para obtener más información acerca de las reglas de contraseñas de las políticas de TI, descargue la hoja de cálculo de referencia de políticas.

Establecimiento de los requisitos de la contraseña de Android

Hay cuatro grupos de reglas de políticas de TI en las contraseñas Android. El grupo de reglas que se utilice depende del tipo de activación del dispositivo y si se van a establecer requisitos para la contraseña del dispositivo o para la contraseña del espacio de trabajo.

Después de establecer las reglas de contraseña en la política de TI, utilice un perfil de conformidad para aplicar los requisitos de contraseña.

Tipo de activación	Compatibilidad con las reglas para la contraseña
Trabajo y personal: privacidad de usuario (Android Enterprise) y Trabajo y personal: control total (Android Enterprise)	Utilice las reglas para contraseñas globales para establecer los requisitos de la contraseña del dispositivo. Utilice las reglas para la contraseña de los perfiles de trabajo para establecer los requisitos de la contraseña del espacio de trabajo. El dispositivo ignora las reglas de contraseña de Knox.
Solo espacio de trabajo (Android Enterprise)	Utilice las reglas para contraseñas globales para establecer los requisitos de la contraseña del dispositivo. Puesto que el dispositivo solo cuenta con un espacio de trabajo, la contraseña también es la contraseña del espacio de trabajo. El dispositivo ignora el resto de las reglas para la contraseña.
Controles de MDM	Utilice las reglas para contraseñas globales para establecer los requisitos de la contraseña del dispositivo. El dispositivo ignora el resto de las reglas para la contraseña. **Nota:** El tipo de activación Controles de MDM está obsoleto en los dispositivos con Android 10. Para obtener más información, https://support.blackberry.com/community para leer el artículo 48386.

Tipo de activación	Compatibilidad con las reglas para la contraseña
Controles de MDM (Samsung Knox)	Utilice las reglas de contraseña de Knox MDM para establecer los requisitos de contraseña del dispositivo. El dispositivo ignora el resto de las reglas para la contraseña.
Trabajo y personal: privacidad de usuario (Samsung Knox)	No tiene ningún control sobre la contraseña del dispositivo. Utilice las reglas de contraseña Knox Premium - Workspace para establecer los requisitos de contraseña del espacio de trabajo. El dispositivo ignora el resto de las reglas para la contraseña. **Nota:** Los tipos de activación de Samsung Knox quedarán en desuso en una versión futura. Los dispositivos compatibles con Knox Platform for Enterprise se pueden activar mediante los tipos de activación de Android Enterprise. Para obtener más información, visite https://support.blackberry.com/community para leer el artículo 54614.
Trabajo y personal: control total (Samsung Knox)	Utilice las reglas de contraseña de Knox MDM para establecer los requisitos de contraseña del dispositivo. Utilice las reglas de contraseña Knox Premium - Workspace para establecer los requisitos de contraseña del espacio de trabajo. El dispositivo ignora el resto de las reglas para la contraseña.
Solo espacio de trabajo (Samsung Knox)	Utilice las reglas de contraseña Knox Premium - Workspace para establecer los requisitos de contraseña del espacio de trabajo. El dispositivo ignora el resto de las reglas para la contraseña.

Android: reglas de contraseñas globales

Las reglas para la contraseña globales establecen los requisitos de la contraseña del dispositivo para los dispositivos con los siguientes tipos de activación:

- Trabajo y personal: privacidad de usuario (Android Enterprise)
- Trabajo y personal: control total (Android Enterprise)
- Solo espacio de trabajo (Android Enterprise)
- Controles de MDM (sin Samsung Knox)

Nota: El tipo de activación de Controles de MDM está obsoleto en los dispositivos con Android 10. Para obtener más información, https://support.blackberry.com/community para leer el artículo 48386.

Regla	Descripción
Complejidad de la contraseña (Global (todos los dispositivos Android))	Especifique el nivel máximo de complejidad de la contraseña del dispositivo. Puede elegir una de las siguientes opciones: • Baja: permite patrones y códigos PIN con valores repetidos o secuenciales. • Media: requiere códigos PIN sin valores repetidos o secuenciales y una longitud mínima de cuatro caracteres o una contraseña con una longitud mínima de cuatro caracteres. • Alta: requiere códigos PIN sin valores repetidos o secuenciales y una longitud mínima de ocho caracteres o una contraseña con una longitud mínima de seis caracteres. **Nota:** Si establece la complejidad de la contraseña en Alta y, a continuación, establece la complejidad de la contraseña en Media en la sección Perfil de trabajo (todos los dispositivos Android) de la política de TI, la configuración global tiene prioridad sobre la configuración del perfil de trabajo y los usuarios se verán obligados a establecer una contraseña de alta complejidad.
Requisitos de la contraseña	Especifique los requisitos mínimos de la contraseña. Puede elegir una de las siguientes opciones: • Sin especificar: no se requiere contraseña • Algunos: el usuario deberá establecer una contraseña pero no habrá requisitos relacionados con la longitud o la calidad • Numérica: la contraseña deberá incluir al menos un número • Alfabética: la contraseña deberá incluir al menos una letra • Alfanumérica: la contraseña deberá incluir al menos una letra y un número • Complejos: permite establecer requisitos específicos para los diferentes tipos de caracteres
Complejidad de la contraseña (perfil de trabajo (todos los dispositivos Android))	Especifique el nivel máximo de complejidad de la contraseña del dispositivo. Puede elegir una de las siguientes opciones: • Baja: permite patrones y códigos PIN con valores repetidos o secuenciales. • Media: requiere códigos PIN sin valores repetidos o secuenciales y una longitud mínima de cuatro caracteres o una contraseña con una longitud mínima de cuatro caracteres. • Alta: requiere códigos PIN sin valores repetidos o secuenciales y una longitud mínima de ocho caracteres o una contraseña con una longitud mínima de seis caracteres. **Nota:** Si establece la complejidad de la contraseña en Media o Baja y ya ha establecido la complejidad de la contraseña en Alta en la sección Global (todos los dispositivos Android) de la política de TI, la configuración global tiene prioridad sobre la configuración del perfil de trabajo y los usuarios se verán obligados a establecer una contraseña de alta complejidad.

Regla	Descripción
Número máximo de intentos de contraseña fallidos	Especifique el número de veces que un usuario puede introducir una contraseña incorrecta antes de que el dispositivo se desactive o se eliminen sus datos. Se eliminan los dispositivos con el tipo de activación "Controles de MDM". Se desactivarán los dispositivos con los tipos de activación "Trabajo y personal: privacidad de usuario " y "Trabajo y personal: privacidad de usuario (Premium)" y se eliminará el perfil de trabajo.
Bloqueo de tiempo de inactividad máximo	Especifique el número máximo de minutos de inactividad del usuario que deben transcurrir antes de que el dispositivo o el espacio de trabajo se bloqueen. En dispositivos Android con un perfil de trabajo, el espacio de trabajo también se bloquea. Los usuarios pueden establecer un periodo más breve en el dispositivo. Esta regla se ignora si no se necesita contraseña.
Tiempo de espera de caducidad de la contraseña	Especifique la cantidad máxima de tiempo que puede utilizarse la contraseña. Una vez transcurrida la cantidad de tiempo especificada, el usuario deberá establecer una nueva contraseña. Si se establece en 0, la contraseña no caduca.
Restricción del historial de contraseñas	Especifique el número máximo de contraseñas anteriores que el dispositivo debe comprobar para evitar que un usuario vuelva a utilizar una contraseña numérica, alfabética, alfanumérica o compleja reciente. Si se establece en 0, el dispositivo no comprueba las contraseñas anteriores.
Longitud mínima de la contraseña:	Especifique el número mínimo de caracteres necesarios en una contraseña numérica, alfabética, alfanumérica o compleja.
Número mínimo de letras mayúsculas requerido en la contraseña	Especifique el número mínimo de letras mayúsculas que debe contener una contraseña compleja.
Número mínimo de letras minúsculas requerido en la contraseña	Especifique el número mínimo de letras minúsculas que debe contener una contraseña compleja.
Número mínimo de letras requerido en la contraseña	Especifique el número mínimo de letras que debe contener una contraseña compleja.
Número mínimo de caracteres no alfabéticos en la contraseña	Especifique el número mínimo de caracteres no alfabéticos (números o símbolos) que debe contener una contraseña compleja.
Mínimo de dígitos numéricos requeridos en la contraseña	Especifique el número mínimo de números que debe contener una contraseña compleja.
Número mínimo de símbolos requerido en la contraseña	Especifique el número mínimo de caracteres complejos que debe contener una contraseña compleja.

Para obtener más información acerca de las reglas de contraseñas de las políticas de TI, descargue la hoja de cálculo de referencia de políticas.

Android: reglas para las contraseñas de los perfiles de trabajo

Las reglas para las contraseñas de los perfiles de trabajo establecen los requisitos de la contraseña del espacio de trabajo para los dispositivos con los siguientes tipos de activación:

- Trabajo y personal: privacidad de usuario (Android Enterprise)
- Trabajo y personal: control total (Android Enterprise)

Regla	Descripción
Requisitos de la contraseña	Especifique los requisitos mínimos de la contraseña del espacio de trabajo. Puede elegir una de las siguientes opciones: • Algunos: el usuario deberá establecer una contraseña pero no habrá requisitos relacionados con la longitud o la calidad • Numérica: la contraseña deberá incluir al menos un número • Alfabética: la contraseña deberá incluir al menos una letra • Alfanumérica: la contraseña deberá incluir al menos una letra y un número • Complejos: permite establecer requisitos específicos para los diferentes tipos de caracteres • Complejos, numérica: la contraseña debe contener caracteres numéricos con secuencias no repetidas (4444) ni ordenadas (1234, 4321, 2468). • Parámetros biométricos débiles: la contraseña permite la tecnología de reconocimiento biométrico de seguridad baja. Para dispositivos con BlackBerry alimentados por Android, puede forzar el espacio de trabajo y las contraseñas de los dispositivos para que sean diferentes mediante la regla "Forzar el espacio de trabajo y las contraseñas de los dispositivos para que sean diferentes" de los dispositivos con BlackBerry.
Número máximo de intentos de contraseña fallidos	Especifique el número de veces que un usuario puede introducir una contraseña incorrecta del espacio de trabajo para que se desactive el dispositivo y el perfil de trabajo se elimine.
Bloqueo de tiempo de inactividad máximo	Especifique cuántos minutos de inactividad del usuario deben transcurrir como máximo para que el dispositivo y el espacio de trabajo se bloqueen. Si configura esta regla y la regla "Bloqueo de tiempo de inactividad máximo" de Android global, el dispositivo y el espacio de trabajo se bloquean cuando el contador de cualquiera de las reglas llega a su fin. Los usuarios pueden establecer un periodo más breve en el dispositivo.
Tiempo de espera de caducidad de la contraseña	Especifique la cantidad máxima de tiempo que puede utilizarse la contraseña del espacio de trabajo. Una vez transcurrida la cantidad de tiempo especificada, el usuario deberá establecer una nueva contraseña del espacio de trabajo. Si se establece en 0, la contraseña no caduca.
Restricción del historial de contraseñas	Especifique el número máximo de contraseñas anteriores del espacio de trabajo que el dispositivo debe comprobar para evitar que un usuario vuelva a utilizar una contraseña numérica, alfabética, alfanumérica o compleja reciente. Si se establece en 0, el dispositivo no comprueba las contraseñas anteriores.

Regla	Descripción
Longitud mínima de la contraseña:	Especifique el número mínimo de caracteres necesarios en una contraseña del espacio de trabajo numérica, alfabética, alfanumérica o compleja.
Número mínimo de letras mayúsculas requerido en la contraseña	Especifique el número mínimo de letras en mayúscula que debe contener la contraseña compleja del espacio de trabajo.
Número mínimo de letras minúsculas requerido en la contraseña	Especifique el número mínimo de letras en minúscula que debe contener la contraseña compleja del espacio de trabajo.
Número mínimo de letras requerido en la contraseña	Especifique el número mínimo de letras que debe contener la contraseña compleja del espacio de trabajo.
Número mínimo de caracteres no alfabéticos en la contraseña	Especifique el número mínimo de caracteres no alfabéticos (números o símbolos) que debe contener una contraseña compleja del espacio de trabajo.
Mínimo de dígitos numéricos requeridos en la contraseña	Especifique el número mínimo de números que debe contener la contraseña compleja del espacio de trabajo.
Número mínimo de símbolos requerido en la contraseña	Especifique el número mínimo de caracteres no alfanuméricos que debe contener una contraseña compleja del espacio de trabajo.
Forzar el uso de contraseñas distintas para el perfil de trabajo y el dispositivo	Especifique si los usuarios deben establecer contraseñas diferentes para el dispositivo y el perfil de trabajo. Cuando las contraseñas son las mismas, al desbloquear el dispositivo se desbloquea el perfil de trabajo.

Para obtener más información acerca de las reglas de contraseñas de las políticas de TI, descargue la hoja de cálculo de referencia de políticas.

Android: reglas para la contraseña de Knox MDM

Las reglas para la contraseña de Knox MDM establecen los requisitos de la contraseña del dispositivo para los dispositivos con los siguientes tipos de activación:

- Trabajo y personal: control total (Samsung Knox)
- Controles de MDM (Knox MDM)

Los dispositivos con estos tipos de activación deben tener una contraseña para el dispositivo.

Si desea activar dispositivos con tipos de activación de Android Enterprise para utilizar Knox Platform for Enterprise, utilice las reglas para las contraseñas de Android global. Los tipos de activación de Samsung Knox y las reglas de políticas de TI de Knox MDM quedarán en desuso en una versión futura. Para obtener más información, https://support.blackberry.com/community y lea el artículo 54614.

Nota: El tipo de activación de Controles de MDM está obsoleto en los dispositivos con Android 10. Para obtener más información, https://support.blackberry.com/community y lea el artículo 48386.

Regla	Descripción
Requisitos de la contraseña	Especifique los requisitos mínimos de la contraseña. Puede elegir una de las siguientes opciones: • Numérica: la contraseña deberá incluir al menos un número • Alfabética: la contraseña deberá incluir al menos una letra • Alfanumérica: la contraseña deberá incluir al menos una letra y un número • Complejos: permite establecer requisitos específicos para los diferentes tipos de caracteres
Longitud mínima de la contraseña:	Especifique la longitud mínima de la contraseña. La contraseña debe tener al menos 4 caracteres.
Número mínimo de letras minúsculas requerido en la contraseña	Especifique el número mínimo de letras minúsculas que debe contener una contraseña compleja.
Número mínimo de letras mayúsculas requerido en la contraseña	Especifique el número mínimo de letras mayúsculas que debe contener una contraseña compleja.
Mínimo de caracteres complejos requeridos en la contraseña	Especifique el número mínimo de caracteres complejos (por ejemplo, números y símbolos) que debe contener una contraseña compleja. Si establece este valor en 1, entonces se requerirá al menos un número. Si establece un valor superior a 1, se requerirán al menos un número y un símbolo.
Longitud de la secuencia máxima de caracteres	Especifique la longitud máxima de una secuencia alfabética permitida en una contraseña alfanumérica o compleja. Por ejemplo, si la longitud de la secuencia alfabética se establece en 5, la secuencia "abcde" estará permitida, pero no la secuencia "abcdef". Si se establece en 0, no habrá restricciones para las secuencias alfabéticas.
Bloqueo de tiempo de inactividad máximo	Especifique el periodo máximo de inactividad del usuario que debe transcurrir antes de que el dispositivo se bloquee (bloqueo protegido con clave). Si el dispositivo se gestiona por varias soluciones EMM, este utilizará el valor más bajo como periodo de inactividad. Si el dispositivo utiliza una contraseña, el usuario deberá proporcionar la contraseña para desbloquear el dispositivo. Si se establece en 0, el dispositivo no contará con un tiempo de espera de inactividad.
Número máximo de intentos de contraseña fallidos	Especifique el número de veces que un usuario puede introducir una contraseña incorrecta antes de que se eliminen los datos del dispositivo.
Restricción del historial de contraseñas	Especifique el número máximo de contraseñas anteriores que el dispositivo debe comprobar para evitar que un usuario vuelva a utilizar una contraseña reciente. Si se establece en 0, el dispositivo no comprueba las contraseñas anteriores.
Tiempo de espera de caducidad de la contraseña	Especifique la cantidad máxima de tiempo que puede utilizarse la contraseña del dispositivo. Una vez transcurrida la cantidad de tiempo especificada, la contraseña caducará y el usuario deberá establecer una nueva contraseña. Si se establece en 0, la contraseña no caduca.

Regla	Descripción
Permitir visibilidad de la contraseña	Especifique si desea que la contraseña del dispositivo pueda ser visible cuando el usuario la escriba. Si no se selecciona esta regla, los usuarios y las aplicaciones de terceros no podrán modificar la configuración de visibilidad.
Permitir la autenticación mediante huella digital	Especifique si el usuario puede usar autenticación de huella digital para el dispositivo.

Para obtener más información acerca de las reglas de contraseñas de las políticas de TI, descargue la hoja de cálculo de referencia de políticas.

Android: reglas para la contraseña de Knox Premium - Workspace

Las reglas para la contraseña de Knox Premium - Workspace establecen los requisitos de la contraseña del espacio de trabajo para los dispositivos con los siguientes tipos de activación:

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

Los dispositivos con estos tipos de activación deben tener una contraseña del espacio de trabajo.

Si desea activar dispositivos con tipos de activación de Android Enterprise para utilizar Knox Platform for Enterprise, utilice las reglas para las contraseñas para perfiles de trabajo de Android. Los tipos de activación de Samsung Knox y las reglas de políticas de TI de Knox Premium quedarán en desuso en una versión futura. Para obtener más información, https://support.blackberry.com/community y lea el artículo 54614.

Regla	Descripción
Requisitos de la contraseña	Especifique los requisitos mínimos de la contraseña. Puede elegir una de las siguientes opciones: • Numérica: la contraseña deberá incluir al menos un número • "Complejos, numérica": la contraseña deberá incluir al menos un número con secuencias no repetidas (4444) ni ordenadas (1234, 4321, 2468) • Alfabética: la contraseña deberá incluir al menos una letra • Alfanumérica: la contraseña deberá incluir al menos una letra y un número • Complejos: permite establecer requisitos específicos para los diferentes tipos de caracteres
Número mínimo de letras minúsculas requerido en la contraseña	Especifique el número mínimo de letras minúsculas que debe contener una contraseña compleja.
Número mínimo de letras mayúsculas requerido en la contraseña	Especifique el número mínimo de letras mayúsculas que debe contener una contraseña compleja.
Mínimo de caracteres complejos requeridos en la contraseña	Especifique el número mínimo de caracteres complejos (por ejemplo, números y símbolos) que debe contener una contraseña compleja. Al menos se requieren tres caracteres complejos, que incluyan al menos un número y un símbolo.

Regla	Descripción
Longitud de la secuencia máxima de caracteres	Especifique la longitud máxima de una secuencia alfabética permitida en una contraseña alfanumérica o compleja. Por ejemplo, si la longitud de la secuencia alfabética se establece en 5, la secuencia "abcde" estará permitida, pero no la secuencia "abcdef". Si se establece en 0, no habrá restricciones para las secuencias alfabéticas.
Longitud mínima de la contraseña:	Especifique la longitud mínima de la contraseña. Si introduce un valor que es menor que el mínimo requerido por Knox Workspace, se utiliza el mínimo Knox Workspace.
Bloqueo de tiempo de inactividad máximo	Especifique el periodo de inactividad máximo del usuario en el espacio de trabajo que debe transcurrir antes de que se bloquee el espacio de trabajo. Si se establece en 0, el espacio de trabajo no contará con un tiempo de espera de inactividad.
Número máximo de intentos de contraseña fallidos	Especifique el número de veces que un usuario puede introducir una contraseña incorrecta antes de que se eliminen los datos del espacio de trabajo. Si se establece en 0, no habrá restricciones en el número de veces que un usuario puede introducir una contraseña incorrecta.
Restricción del historial de contraseñas	Especifique el número máximo de contraseñas anteriores que el dispositivo debe comprobar para evitar que un usuario vuelva a utilizar una contraseña reciente. Si se establece en 0, el dispositivo no comprueba las contraseñas anteriores.
Tiempo de espera de caducidad de la contraseña	Especifique el número máximo de días que puede utilizarse la contraseña. Una vez transcurrido el número de días especificado, la contraseña caducará y el usuario deberá establecer una nueva contraseña. Si se establece en 0, la contraseña no caduca.
Número mínimo de caracteres modificados para las nuevas contraseñas	Especifique el número mínimo de caracteres modificados que debe incluir una nueva contraseña en comparación con la contraseña anterior. Si se establece en 0, no se aplican restricciones.
Permitir personalización de la clave de bloqueo	Especifique si un dispositivo puede utilizar la personalización de la clave de bloqueo, como los agentes de confianza. Si no se selecciona esta regla, la personalización de la clave de bloqueo se desactivará.
Permitir agentes de confianza de la clave de bloqueo	Especifique si un usuario puede mantener el espacio de trabajo desbloqueado durante 2 horas después del tiempo de espera máximo de inactividad. Si no establece un valor para el tiempo de inactividad, el usuario podrá realizar esta acción de forma predeterminada.
Permitir visibilidad de la contraseña	Especifique si desea que la contraseña del dispositivo pueda ser visible cuando el usuario la escriba. Si no se selecciona esta regla, los usuarios y las aplicaciones de terceros no podrán modificar la configuración de visibilidad.
Ejecutar autenticación de dos factores	Especifique si un usuario debe utilizar la autenticación en dos fases para acceder al espacio de trabajo. Por ejemplo, puede utilizar esta regla si desea que el usuario se autentique utilizando una huella digital y una contraseña.

Regla	Descripción
Permitir la autenticación mediante huella digital	Especifique si el usuario puede usar la autenticación mediante huella digital para acceder al espacio de trabajo.

Para obtener más información acerca de las reglas de contraseñas de las políticas de TI, descargue la hoja de cálculo de referencia de políticas.

Establecimiento de los requisitos de la contraseña de Windows 10

Puede elegir si los dispositivos Windows 10 deben tener una contraseña. Si se requiere una contraseña, puede establecer los requisitos para esta.

Regla	Descripción
Se requiere contraseña para el dispositivo	Especifique si el usuario debe establecer una contraseña para el dispositivo.
Permitir contraseña sencilla	Especifique si la contraseña puede contener caracteres repetidos o secuenciales, como DEFG o 3333.
Longitud mínima de la contraseña:	Especifique la longitud mínima de la contraseña. La contraseña debe tener al menos 4 caracteres.
Complejidad de la contraseña	Especifique la complejidad de la contraseña. Puede elegir las siguientes opciones: • Alfanumérica: la contraseña deberá contener letras y números • Numérica: la contraseña deberá contener solo números
Número mínimo de tipos de caracteres	Especifique el número mínimo de tipos de caracteres que debe contener una contraseña alfanumérica. Seleccione de entre las siguientes opciones: **1.** números necesarios **2.** números y letras en minúscula necesarios **3.** números, letras mayúsculas y letras minúsculas necesarios **4.** números, letras mayúsculas y letras minúsculas y caracteres especiales necesarios Los requisitos de caracteres de contraseña para equipos y tabletas con Windows 10 se determinan en función del tipo de cuenta de usuario, no de esta configuración.
Caducidad de la contraseña	Especifique el número máximo de días que puede utilizarse la contraseña. Si se establece en 0, la contraseña no caduca.
Historial de contraseñas	Especifique el número de contraseñas anteriores que el dispositivo debe comprobar para evitar que un usuario vuelva a utilizar una contraseña reciente. Si se establece en 0, el dispositivo no comprueba las contraseñas anteriores.

Regla	Descripción
Número máximo de intentos de contraseña fallidos	Especifique el número de veces que un usuario puede introducir una contraseña incorrecta antes de que se eliminen los datos del dispositivo. Si se establece en 0, no se eliminarán los datos del dispositivo con independencia de las veces que el usuario haya introducido una contraseña incorrecta. Esta regla no se aplica a los dispositivos que permiten varias cuentas de usuario, incluyendo los equipos y tabletas con Windows 10.
Bloqueo de tiempo de inactividad máximo	Especifique el periodo de inactividad del usuario que debe transcurrir antes de que el dispositivo se bloquee. Si se establece en 0, el dispositivo no se bloquea automáticamente.
Permitir salir del estado inactivo sin contraseña	Especifique si un usuario debe escribir la contraseña una vez que termine el periodo de gracia de la inactividad. Si se selecciona esta regla, el usuario podrá establecer el temporizador del periodo de gracia de la contraseña en el dispositivo. Esta regla no se aplica a equipos y tabletas Windows 10.

Para obtener más información acerca de las reglas de contraseñas de las políticas de TI, descargue la hoja de cálculo de referencia de políticas.

Creación y gestión de políticas de TI

Puede utilizar la política de TI predeterminada o crear políticas de TI personalizadas (por ejemplo, para especificar reglas de políticas de TI de diferentes grupos de usuarios o de dispositivos en la empresa). Si va a utilizar la política de TI predeterminada, debería revisarla y, si fuera necesario, actualizarla para asegurarse de que las reglas cumplan con los estándares de seguridad de la empresa.

Creación de una política de TI

1. En la barra de menú, haga clic en **Políticas y perfiles**.
2. Haga clic en **Política > Políticas de TI**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para la política de TI.
5. Haga clic en la pestaña para cada tipo de dispositivo en la empresa y configure los valores apropiados para las reglas de políticas de TI.

   Mantenga el ratón sobre el nombre de una regla para mostrar sugerencias de ayuda.
6. Haga clic en **Agregar**.

Después de terminar: Clasificar políticas de TI

Copie una política de TI

Puede copiar las políticas de TI actuales para crear rápidamente políticas de TI personalizadas para los distintos grupos de la empresa.

1. En la barra de menú, haga clic en **Políticas y perfiles**.
2. Haga clic en **Política > Políticas de TI**.
3. Haga clic en el nombre de la política de TI que desea copiar.

4. Haga clic en  .
5. Escriba un nombre y una descripción para la nueva política de TI.
6. Realice modificaciones en la pestaña adecuada para cada tipo de dispositivo.
7. Haga clic en **Agregar**.

Después de terminar: Clasificar políticas de TI

Clasificar políticas de TI

La clasificación se utiliza para determinar la política de TI que BlackBerry UEM envía a un dispositivo en las situaciones siguientes:

- Un usuario es miembro de varios grupos de usuarios que tienen diferentes políticas de TI.
- Un dispositivo es miembro de varios grupos de dispositivos que tienen diferentes políticas de TI.

1. En la barra de menú, haga clic en **Políticas y perfiles**.
2. Haga clic en **Política > Políticas de TI**.
3. Haga clic en .
4. Utilice las flechas para mover las políticas de TI hacia arriba o hacia abajo en la clasificación.
5. Haga clic en **Guardar**.

Presentación de políticas de TI

Puede ver la siguiente información acerca de una política de TI:

- Reglas de políticas de TI específicas para cada tipo de dispositivo
- La lista y el número de cuentas de usuario a las que la política de TI está asignada (directa e indirectamente)
- La lista y el número de grupos de usuarios a los que la política de TI está asignada (directamente)

1. En la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Política > Políticas de TI**.
3. Haga clic en el nombre de la política de TI que desea ver.

Cambiar una política de TI

1. En la barra de menú, haga clic en **Políticas y perfiles**.
2. Haga clic en **Política > Políticas de TI**.
3. Haga clic en el nombre de la política de TI que desee cambiar.
4. Haga clic en  .
5. Realice modificaciones en la pestaña adecuada para cada tipo de dispositivo.
6. Haga clic en **Guardar**.

Después de terminar: Si es necesario, cambie la clasificación de la política de TI.

Eliminación de una política de TI de las cuentas o de los grupos de usuarios

Si una política de TI se asigna directamente a las cuentas o los grupos de usuarios, puede eliminarla. Si a un grupo de usuarios se asigna directamente una política de TI, se podrá eliminar la política de TI o las cuentas de usuario del grupo. Al eliminar una política de TI de los grupos de usuarios, se eliminará la política de TI de cada usuario que pertenezca a los grupos seleccionados.

Nota: La política de TI predeterminada solo se puede eliminar de una cuenta de usuario si se ha asignado directamente al usuario.

1. En la barra de menú, haga clic en **Políticas y perfiles**.
2. Haga clic en **Política > Políticas de TI**.
3. Haga clic en el nombre de la política de TI que desea eliminar de las cuentas o grupos de usuarios.
4. Lleve a cabo una de las tareas siguientes:

Tarea	Pasos
Eliminar una política de TI de las cuentas de usuario	**a.** Haga clic en la pestaña **Asignación para usuarios**. **b.** Si es necesario, busque cuentas de usuario. **c.** Seleccione las cuentas de usuario de las que desea eliminar de la política de TI. **d.** Haga clic en .
Eliminar una política de TI de los grupos de usuarios	**a.** Haga clic en la pestaña **Asignación para grupos**. **b.** Si es necesario, busque grupos de usuarios. **c.** Seleccione los grupos de usuarios de los que desea eliminar la política de TI. **d.** Haga clic en .

Eliminar una política de TI

No puede eliminar la política de TI predeterminada. Cuando se elimina una política de TI personalizada, BlackBerry UEM elimina la política de TI de los usuarios y dispositivos a los que está asignada.

1. En la barra de menú, haga clic en **Políticas y perfiles**.
2. Haga clic en **Política > Políticas de TI**.
3. Seleccione las casillas de verificación de las políticas de TI que desea eliminar.
4. Haga clic en .
5. Haga clic en **Eliminar**.

Exporte las políticas de TI

Puede exportar las políticas de TI a un archivo .xml para fines de auditoría.

Nota:

Los perfiles que están asociados a las políticas de TI no se exportan.

1. En la barra de menú, haga clic en **Políticas y perfiles**.
2. Haga clic en **Política > Políticas de TI**.
3. Seleccione las casillas de verificación de las políticas de TI que desea exportar.
4. Haga clic en .
5. Haga clic en **Siguiente**.
6. Haga clic en **Exportar**.

¿Cómo elige BlackBerry UEM qué política de TI asignar?

BlackBerry UEM envía una sola política de TI a un dispositivo y utiliza reglas predefinidas para determinar la política de TI que se asigna a un usuario y a los dispositivos que el usuario activa.

Asignado a	Reglas
Cuenta de usuario (ver pestaña Resumen)	**1.** Una política de TI asignada directamente a una cuenta de usuario tiene prioridad sobre una política de TI asignada indirectamente por grupo de usuarios. **2.** Si un usuario es miembro de varios grupos de usuarios que tienen políticas de TI diferentes, BlackBerry UEM asigna la política de TI con la clasificación más alta. **3.** La política de TI predeterminada se asigna si no hay otra que esté asignada directamente a una cuenta de usuario o a través de la pertenencia a un grupo de usuarios.
Dispositivo (ver pestaña Dispositivo)	De forma predeterminada, un dispositivo hereda la política de TI que BlackBerry UEM asigna al usuario que lo activa. Si un dispositivo pertenece a un grupo de dispositivos, se aplican las siguientes reglas: **1.** Una política de TI asignada a un grupo de dispositivos tiene prioridad sobre la política de TI que BlackBerry UEM asigna a un grupo de usuarios. **2.** Si un dispositivo es miembro de varios grupos de dispositivos que tienen políticas de TI diferentes, BlackBerry UEM asigna la política de TI con la clasificación más alta.

BlackBerry UEM puede tener que resolver los conflictos de las políticas de TI cuando se realicen alguna de las siguientes acciones:

- Asignación de una política de TI a una cuenta de usuario, a un grupo de usuarios o a un grupo de dispositivos
- Eliminación de una política de TI de una cuenta de usuario, a un grupo de usuarios o a un grupo de dispositivos
- Cambio de la clasificación de la política de TI
- Eliminar una política de TI
- Cambiar la pertenencia a grupos de usuarios (cuentas de usuario y grupos anidados)
- Cambio de los atributos del dispositivo
- Cambio de la pertenencia a un grupo de dispositivos
- Eliminación de un grupo de usuarios o de un grupo de dispositivos

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

BlackBerry Envía periódicamente actualizaciones de las políticas de TI y los metadatos de dispositivos a instalaciones de BlackBerry UEM con el fin de proporcionar información sobre actualizaciones de la mano de proveedores de dispositivos y SO.

Por ejemplo, después de que el proveedor del dispositivo publique un nuevo modelo del dispositivo,BlackBerry puede enviar metadatos actualizados de los dispositivos a las instalaciones de BlackBerry UEM para que los perfiles de activación y conformidad incluyan el nuevo modelo del dispositivo y pueda admitirse o restringirse en el perfil. Cuando Apple, Google o Microsoft presenten actualizaciones de SO, se enviará un nuevo conjunto de políticas de TI a las instalaciones de UEM de BlackBerry UEM para permitirle controlar las nuevas funciones de la actualización de SO.

De forma predeterminada, BlackBerry UEM instala estas actualizaciones automáticamente. Si la política de seguridad de su empresa no permitiera actualizaciones automáticas, puede desactivarlas e importar actualizaciones en BlackBerry UEM de forma manual.

También puede configurar notificaciones de eventos para informar a los administradores cuando se instalen actualizaciones de políticas de TI y metadatos de dispositivos.

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

BlackBerry envía notificaciones cuando hay nuevas actualizaciones disponibles. 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.

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

1. En la barra de menús, haga clic en **Configuración**.
2. Haga clic en **Infraestructura > Importar datos de configuración**.
3. Realice una de las acciones siguientes, o ambas:
   - Para desactivar las actualizaciones automáticas de los conjuntos de políticas de TI, desmarque la casilla **Actualizar automáticamente datos de conjuntos de políticas de TI**.
   - Para desactivar las actualizaciones automáticas de los metadatos de dispositivos, desmarque la casilla **Actualizar automáticamente metadatos de dispositivos**.
4. Haga clic en el botón **Explorar** correspondiente para encontrar el archivo de datos que quiere importar y, cuando lo haya localizado, haga clic en **Abrir**.

Creación de mensajes de ayuda del dispositivo

En dispositivos con 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.

También puede especificar un mensaje de ayuda de administrador que se muestra en la pantalla de configuración Administraciones del dispositivo. Por ejemplo, puede que desee mostrar un aviso de que su empresa puede supervisar y gestionar aplicaciones y datos en el perfil de trabajo.

Si su empresa cuenta con usuarios que trabajan en más de un idioma, puede agregar mensajes de ayuda en idiomas adicionales y especificar el idioma predeterminado que se muestra en los dispositivos que no utilizan uno de los idiomas disponibles.

Crear mensajes de ayuda del dispositivo

Los mensajes de ayuda del dispositivo son compatibles con dispositivos con Android 8.0 y versiones posteriores.

1. En la barra de menús, haga clic en **Configuración > Configuración general**.
2. Haga clic en **Mensajes de ayuda del dispositivo personalizados**.
3. En la pestaña **Mensajes de ayuda del dispositivo personalizados**, haga clic en **Agregar**.
4. Seleccione el idioma en el que desea que aparezca la notificación.
5. En el campo **Aviso de funciones desactivada**, escriba el aviso que desea mostrar en el dispositivo cuando una función está desactivada. El mensaje puede tener hasta 200 caracteres.
6. Opcionalmente, en el campo **Mensaje de ayuda de administrador**, escriba un aviso para que se muestre en la pantalla de configuración Administradores del dispositivo.
7. Si desea crear un mensaje en más de un idioma, haga clic en **Agregar un idioma adicional** y repita los pasos del 4 al 6 para cada idioma.
8. Si ha agregado mensajes en más de un idioma, seleccione **Idioma predeterminado** junto al idioma que desea que aparezca en los dispositivos que no utilizan uno de los idiomas disponibles. Por ejemplo, si los idiomas disponibles son inglés y francés, e inglés es el idioma predeterminado, el mensaje en inglés parecerá en los dispositivos que utilicen alemán.
9. 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 cumplimiento especifica la información siguiente:

- Condiciones que podrían hacer que un dispositivo no cumpla los requisitos.
- Los mensajes de correo electrónico y las notificaciones de dispositivos que reciben los usuarios si infringen las condiciones de conformidad.
- Acciones que se realizan si los usuarios no corrigen el problema, que incluyen la limitación del acceso de un usuario a los recursos de la empresa, la eliminación de datos de trabajo del dispositivo o de todos los datos de dicho dispositivo.

En los dispositivos Samsung Knox, puede agregar una lista de las aplicaciones restringidas a un perfil de cumplimiento. Sin embargo, BlackBerry UEM no impone el cumplimiento de las reglas 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.

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

Creación de un perfil de conformidad

Antes de empezar:

- Si define reglas para restringir o permitir aplicaciones específicas, agregue estas aplicaciones a la lista de aplicaciones restringidas. Para obtener más información, consulte Adición de una aplicación a la lista de aplicaciones restringidas. Esto no se aplica a las aplicaciones integradas para dispositivos de 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: configuración del perfil de conformidad.
- Si desea enviar una notificación de correo electrónico a los usuarios cuando sus dispositivos no cumplan, edite el correo electrónico de cumplimiento predeterminado o cree una nueva plantilla de correo electrónico. Para obtener más información, consulte Creación de una plantilla para las notificaciones de conformidad por correo electrónico.

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, haga clic en **Políticas y perfiles**.
2. Haga clic en **Conformidad > Conformidad**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil de cumplimiento.
5. Si desea enviar un mensaje de notificación a los usuarios cuando sus dispositivos no cumplen con los requisitos, realice cualquiera de las acciones siguientes:

- En la lista desplegable **Mensaje de correo electrónico enviado cuando se detecta infracción**, seleccione una plantilla de correo electrónico. Para ver el correo electrónico de cumplimiento predeterminado, haga clic en Configuración > Configuración general > Plantillas de correo electrónico.
- En la lista desplegable **Intervalo de aplicación**, seleccione la frecuencia de las comprobaciones de cumplimiento. Esta configuración solo se aplica a las comprobaciones de cumplimiento de BlackBerry Dynamics. Tenga en cuenta que no puede configurar el intervalo de aplicación para las comprobaciones de cumplimiento de BlackBerry Dynamics, que se producen a intervalos regulares.
- Amplíe **Notificación de dispositivo enviada cuando se detecta una violación de conformidad**. Edite el mensaje si es necesario.

Puede utilizar variables para rellenar las notificaciones con información de los usuarios, del dispositivo y del cumplimiento. Para obtener más información, consulte Variables.

6. 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 Configuración del perfil de conformidad.
7. Haga clic en **Agregar**.

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

Configuración del perfil de conformidad

Los perfiles de conformidad son compatibles con los siguientes tipos de dispositivos:

- iOS
- macOS
- Android
- Windows

Común: configuración del perfil de conformidad

Dispositivos con iOS, iPadOS, y con Android.

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.

Común: configuración del perfil de conformidad	Descripción
Comportamiento de aviso	En la configuración se especifica cómo BlackBerry 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 BlackBerry UEM interviene inmediatamente. Valores posibles: • Aviso sobre conformidad • Acción de conformidad inmediata

Común: configuración del perfil de conformidad	Descripción
Método de aviso	En la configuración se especifica cómo BlackBerry UEM solicita al usuario que corrija un problema de cumplimiento. Valores posibles • Notificación del dispositivo • Notificaciones de correo electrónico y del dispositivo Las aplicaciones de BlackBerry Dynamics no envían notificaciones por correo electrónico a los usuarios. Las aplicaciones de BlackBerry Dynamics solo proporcionan notificaciones del dispositivo, independientemente de esta configuración. Para las reglas de cumplimiento que se aplican al dispositivo, el valor predeterminado es "Notificaciones de correo electrónico y del dispositivo". Para las reglas de cumplimiento que se aplican solo a las aplicaciones de BlackBerry Dynamics, el valor predeterminado es "Notificaciones del dispositivo". Esta configuración solo es válida si "Comportamiento de aviso" está establecida en "Aviso sobre conformidad".
Recuento de avisos	En la configuración se especifica el número de veces que se solicita al usuario que corrija un problema de conformidad. El valor predeterminado es "3". 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. El valor predeterminado es "4 horas". Esta configuración solo es válida si "Comportamiento de aviso" está establecida en "Aviso sobre conformidad".

Común: configuración del perfil de conformidad	Descripción
Acción de cumplimiento para dispositivo	Esta configuración especifica la acción que BlackBerry UEM realiza en dispositivos que no cumplen los requisitos. Valores posibles: • Supervisar y registrar: BlackBerry UEM identifica la infracción de conformidad pero no realiza ninguna acción de cumplimiento en el dispositivo. • No es de confianza: en dispositivos con iOS, iPadOS, macOS, Android, y Windows, esta opción evita que el usuario acceda a aplicaciones y recursos de trabajo desde el dispositivo. Los datos y las aplicaciones no se eliminan del dispositivo. **Nota:** 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: en los dispositivos con iOS, iPadOS,Android y Windows, se puede desactivar un dispositivo de BlackBerry UEM si infringe la regla "Fuera de contacto". El valor predeterminado es "Supervisar y registrar". Esta configuración no es válida para dispositivos activados con Privacidad del usuario. En los dispositivos activados con "Trabajo y personal: privacidad de usuario", no puede eliminar todos los datos del dispositivo del usuario. Si selecciona "Eliminar todos los datos", BlackBerry UEM realiza la misma acción que "Eliminar solo los datos de trabajo". Para los dispositivos con Samsung Knox Workspace que solo cuentan con un espacio de trabajo, si selecciona "Eliminar solo los datos de trabajo", "Eliminar todos los datos" o "Eliminar del servidor", se eliminarán todos los datos del dispositivo. 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 define lo que ocurre con las aplicaciones de BlackBerry Dynamics cuando un dispositivo no está en conformidad. Valores posibles: • No permitir la ejecución de aplicaciones de BlackBerry Dynamics • Eliminar datos de aplicaciones BlackBerry Dynamics • Supervisar y registrar: BlackBerry UEM identifica la infracción de conformidad pero no realiza ninguna acción de cumplimiento El valor predeterminado es "Supervisar y registrar".

Dispositivos Windows 10 y macOS

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.

Común: configuración del perfil de conformidad	Descripción
Acción de cumplimiento	Esta configuración especifica la acción que BlackBerry UEM realiza en dispositivos que no cumplen los requisitos. Valores posibles: • Aviso sobre conformidad • No confiar: en dispositivos con Windows, esta opción evita que el usuario acceda a los recursos y aplicaciones de trabajo desde el dispositivo. Los datos y las aplicaciones no se eliminan del dispositivo. **Nota:** Untrust no es compatible con las aplicaciones de BlackBerry Dynamics. • Eliminar solo los datos de trabajo • Eliminar todos los datos • Eliminar del servidor: en los dispositivos con Windows, se puede desactivar un dispositivo de BlackBerry UEM si infringe la regla "Fuera de contacto". • Ninguna: identifica una infracción de cumplimiento pero no realiza ninguna acción. El valor predeterminado es "Aviso sobre conformidad".
Método de aviso	Los valores posibles son: • Notificación de correo electrónico • Notificación del dispositivo • Ambas El valor predeterminado es "Ambas". Esta configuración solo es válida si "Acción de cumplimiento" está establecida en "Aviso sobre conformidad". Los dispositivos con Windows 10 no son compatibles con las notificaciones de dispositivos.
Recuento de avisos	En la configuración se especifica el número de veces que se solicita al usuario que corrija la infracción. El valor predeterminado es "3". Esta configuración solo es válida si "Acción de cumplimiento" está establecida en "Aviso sobre conformidad".
Intervalo de aviso	En la configuración se especifica el tiempo entre avisos, en minutos, horas o días. El valor predeterminado es "4 horas". Esta configuración solo es válida si "Acción de cumplimiento" está establecida en "Aviso sobre conformidad".

Común: configuración del perfil de conformidad	Descripción
Acción al caducar el intervalo de aviso	Esta configuración define lo que sucede cuando el usuario ha recibido el número total de avisos, tal como se define en Recuento de avisos, y no corrige la infracción. Valores posibles: • Ninguno • No confiar: en dispositivos con Windows, esta opción evita que el usuario acceda a los recursos y aplicaciones de trabajo desde el dispositivo. Los datos y las aplicaciones no se eliminan del dispositivo. **Nota:** Untrust no es compatible con las aplicaciones de BlackBerry Dynamics. Utilice una acción de cumplimiento alternativa. • Eliminar solo los datos de trabajo • Eliminar todos los datos El valor predeterminado es "No es de confianza". Esta configuración solo es válida si "Acción de cumplimiento" está establecida en "Aviso sobre conformidad".
Acción de cumplimiento para las aplicaciones de BlackBerry Dynamics	Esta configuración define lo que ocurre con las aplicaciones de BlackBerry Dynamics cuando un dispositivo no está en conformidad. Valores posibles: • Eliminar datos de aplicaciones BlackBerry Dynamics • No permitir la ejecución de aplicaciones de BlackBerry Dynamics El valor predeterminado es "Eliminar datos de aplicaciones de BlackBerry Dynamics".

iOS: configuración del perfil de conformidad

Consulte Común: configuración del perfil de conformidad para obtener una explicación sobre las acciones posibles si se selecciona una regla de conformidad.

Esta configuración se aplica también a dispositivos con iPadOS.

iOS: 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 tampoco podrán realizar nuevas activaciones para dispositivos liberados, independientemente de la acción de conformidad que haya establecido.

iOS: configuración del perfil de conformidad	Descripción
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 selecciona esta configuración y una aplicación no asignada está instalada en un dispositivo, se muestran un mensaje de advertencia y un enlace en la pestaña Dispositivos gestionados. Al hacer clic en el enlace, se muestra una lista de las aplicaciones que hacen que el dispositivo no cumpla los requisitos de conformidad. Esta configuración no es válida para los dispositivos activados 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. Cuando selecciona esta configuración y una aplicación obligatoria no está instalada en un dispositivo, se muestran un mensaje de advertencia y un enlace en la pestaña Dispositivos gestionados. Al hacer clic en el enlace, se muestra una lista de las aplicaciones que hacen que el dispositivo no cumpla los requisitos de conformidad.
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 elegir una de estas opciones: • Permitir modelos de dispositivo seleccionados • No permitir modelos de dispositivo seleccionados Puede seleccionar 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.
Dispositivo fuera de contacto	Esta configuración crea una regla de conformidad para garantizar que los dispositivos no están fuera de contacto con BlackBerry UEM durante más de un periodo especificado.
Última hora de contacto	Esta configuración especifica el número de días que un dispositivo puede estar fuera de contacto con BlackBerry UEM. Esta configuración es válida únicamente si se ha seleccionado la opción "Dispositivo fuera de contacto".

iOS: configuración del perfil de conformidad	Descripción
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 BlackBerry 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 BlackBerry UEM. Esta configuración solo se aplica si se especifica una delegada de autenticación en un perfil de BlackBerry Dynamics. En la configuración "Hora del último contacto" se especifica el número de días en los que un dispositivo puede estar fuera de contacto con BlackBerry UEM antes de que el dispositivo infrinja 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.
Captura de pantalla de la aplicación de BlackBerry Dynamics detectada	Esta configuración crea una regla de conformidad que reacciona a las capturas de pantalla de las aplicaciones de BlackBerry Dynamics en dispositivos iOS. En el ajuste "Número máximo de capturas de pantalla en un periodo" se especifica el número de capturas de pantalla permitidas en el tiempo especificado en el campo "Duración del periodo". 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.

iOS: configuración del perfil de conformidad	Descripción
La aplicación restringida está instalada	Esta configuración crea una regla de conformidad para que BlackBerry UEM compruebe periódicamente si hay aplicaciones restringidas. Para restringir las aplicaciones, realice cualquiera de las siguientes tareas: • Seleccione una aplicación de la lista de aplicaciones restringidas. Para obtener más información, consulte Adición de una aplicación a la lista de aplicaciones restringidas. Lleve a cabo una de estas acciones: • Para seleccionar aplicaciones mediante el nombre de la aplicación, haga clic en la opción Seleccionar aplicaciones de la lista de aplicaciones. • Para seleccionar aplicaciones utilizando el ID de paquete de aplicación, haga clic en la opción Especifique el ID de paquete de aplicación. No debe utilizar el ID de paquete para agregar aplicaciones públicas. Agregue las aplicaciones públicas a la lista de aplicaciones restringidas y, a continuación, utilice la opción Seleccionar aplicaciones de la lista de aplicaciones para seleccionar las aplicaciones en su lugar. • Seleccione una aplicación integrada (solo para dispositivos supervisados) Para eliminar una aplicación de la lista, haga clic en ✕. Cuando selecciona esta configuración y una aplicación restringida está instalada en un dispositivo, se muestran un mensaje de advertencia y un enlace en la pestaña Dispositivos gestionados. Al hacer clic en el enlace, se muestra una lista de las aplicaciones que hacen que el dispositivo no cumpla los requisitos 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 conformidad que especifica una lista de aplicaciones que se pueden instalar en los dispositivos de los usuarios. El resto de aplicaciones no están permitidas. Para permitir aplicaciones específicas, realice una de las siguientes tareas: • Seleccione una aplicación de la lista de aplicaciones restringidas. Para obtener más información, consulte Adición de una aplicación a la lista de aplicaciones restringidas. • Seleccionar una aplicación integrada Algunas aplicaciones están incluidas en la lista de permitidos de manera predeterminada. Para eliminar una aplicación de la lista, haga clic en ✕. 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 posibles si se selecciona una regla de conformidad.

macOS: 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 cumplimiento que haya establecido.
Modelo de dispositivo restringido detectado	Esta configuración crea una regla de conformidad para restringir modelos de dispositivo. Puede elegir una de estas opciones: • Permitir modelos de dispositivo seleccionados • No permitir modelos de dispositivo seleccionados Puede seleccionar 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 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 BlackBerry 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 BlackBerry 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 en los que un dispositivo puede estar fuera de contacto con BlackBerry UEM antes de que el dispositivo infrinja el cumplimiento.

Android: Configuración del perfil de conformidad

Consulte Común: configuración del perfil de conformidad para obtener una explicación sobre las acciones posibles si se selecciona una regla de conformidad.

Android: Configuración de conformidad	Descripción
Error de atestación de Knox o SO con acceso a la raíz	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. Un dispositivo tiene acceso a la raíz cuando un usuario o atacante obtiene acceso al nivel de raíz del sistema operativo Android. Esta regla se aplica al estado de acceso a la raíz del dispositivo si la atestación de UEM Client, BlackBerry Dynamics SDK o Knox lo detecta. 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. Si establece una regla de conformidad para "Error de atestación de Knox o SO con acceso a la raíz", al seleccionar "Activar antidepuración para las aplicaciones de BlackBerry Dynamics" se detendrán las aplicaciones de BlackBerry Dynamics si el tiempo de ejecución de BlackBerry Dynamics detecta una herramienta de depuración activa.
Error de atestación de SafetyNet	Esta configuración crea una regla de conformidad que especifica las acciones que se producen si los dispositivos no superan la atestación de SafetyNet. Al utilizar la atestación de SafetyNet, BlackBerry UEM realiza comprobaciones para probar la autenticidad e integridad de los dispositivos y aplicaciones de Android de su entorno empresarial. Para que las configuraciones surtan efecto, debe activar la función de atestación de SafetyNet en la consola de gestión en Configuración > Atestación > Frecuencia de atestación de SafetyNet. Para obtener más información acerca de la configuración de atestación de SafetyNet, consulte Configuración de atestaciones de dispositivos Android y aplicaciones de BlackBerry Dynamics mediante SafetyNet.
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 selecciona esta configuración y una aplicación no asignada está instalada en un dispositivo con Android, se muestran un mensaje de advertencia y un enlace en la pestaña Dispositivos gestionados. Al hacer clic en el enlace, se muestra una lista de las aplicaciones que hacen que el dispositivo no cumpla los requisitos de conformidad. Para los dispositivos Android Enterprise 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.

Android: Configuración 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. Cuando selecciona esta configuración y una aplicación obligatoria no está instalada en un dispositivo con Android, se muestran un mensaje de advertencia y un enlace en la pestaña Dispositivos gestionados. Al hacer clic en el enlace, se muestra una lista de las aplicaciones que hacen que el dispositivo no cumpla los requisitos de conformidad. Para los dispositivos Android Enterprise, no se aplican las acciones de conformidad. 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.
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 elegir una de estas opciones: • Permitir modelos de dispositivo seleccionados • No permitir modelos de dispositivo seleccionados 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.
Dispositivo fuera de contacto	Esta configuración crea una regla de conformidad para supervisar si los dispositivos están fuera de contacto con BlackBerry UEM durante más tiempo del especificado. En la configuración "Hora del último contacto" se especifica el número de días durante los que un dispositivo puede estar fuera de contacto con BlackBerry UEM antes de que el dispositivo infrinja la conformidad.

Android: Configuración de conformidad	Descripción
El nivel de revisión de seguridad requerido 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". Esta configuración es válida para dispositivos y aplicaciones de BlackBerry Dynamics desarrollados con BlackBerry Dynamics SDK 6.0 y posterior.
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 comprobar si las aplicaciones de BlackBerry Dynamics están fuera de contacto con BlackBerry UEM durante más tiempo del especificado. La acción de conformidad se aplica a las aplicaciones de BlackBerry Dynamics. En la configuración "Basar intervalo de conectividad en las aplicaciones delegadas de autenticación" se especifica que la verificación de conectividad se basa en el momento en el que se conecta una aplicación delegada de autenticación a BlackBerry UEM. Esta configuración solo se aplica si se especifica una delegada de autenticación en un perfil de BlackBerry Dynamics. En la configuración "Hora del último contacto" se especifica el número de días durante los que un dispositivo puede estar fuera de contacto con BlackBerry UEM antes de que el dispositivo infrinja la conformidad. Las aplicaciones de BlackBerry Dynamics no exigen a los usuarios la conformidad con 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, se restablecerá la conformidad cuando el usuario abra la aplicación de BlackBerry Dynamics.

Android: Configuración de conformidad	Descripción
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, 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 Android Enterprise y Samsung Knox con activaciones Trabajo y personal: control total, seleccione "Ejecutar acciones de conformidad en el espacio personal" para aplicar la regla a las aplicaciones tanto en el perfil de trabajo como en el perfil personal. Esta opción solo es compatible con dispositivos con Android 10 y anterior. Esta configuración no es válida para dispositivos activados con Privacidad del usuario. Cuando selecciona esta configuración y una aplicación restringida está instalada en un dispositivo con Android, se muestran un mensaje de advertencia y un enlace en la pestaña Dispositivos gestionados. Al hacer clic en el enlace, se muestra una lista de las aplicaciones que hacen que el dispositivo no cumpla los requisitos de conformidad. **Nota:** Si ha activado un dispositivo mediante el tipo de activación Android Enterprise - Control total y utiliza esta opción para desactivar las aplicaciones en el lado personal del dispositivo, cuando el dispositivo se actualice de Android 10 a Android 11, dichas aplicaciones se desactivarán de forma permanente a menos que vuelva a activar el dispositivo. Para obtener más información, visite support.blackberry.com/community para leer el artículo 76852.
La contraseña no cumple los requisitos de complejidad	Esta opción crea una regla de conformidad para asegurarse de que las contraseñas definidas por el usuario para el dispositivo o el espacio de trabajo cumplan los requisitos de conformidad definidos en la política de TI que tiene asignada.

Windows: Configuración del perfil de conformidad

Consulte Común: configuración del perfil de conformidad para obtener una explicación sobre las acciones posibles si se selecciona una regla de conformidad.

Windows: 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.

Windows: 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 del SO restringida instalada según se especifica en esta configuración. Puede seleccionar las versiones del SO restringidas.
Modelo de dispositivo restringido detectado	Esta configuración crea una regla de conformidad para restringir modelos de dispositivo según se especifica en esta configuración. Valores posibles: • Permitir modelos de dispositivo seleccionados • No permitir modelos de dispositivo seleccionados 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 BlackBerry 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 BlackBerry UEM durante más de un periodo especificado. La acción de conformidad 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 BlackBerry UEM instalar actualizaciones del sistema operativo Windows o notificar a los usuarios las actualizaciones necesarias.

Windows: Configuración del perfil de conformidad	Descripción
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.
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.

Windows: Configuración del perfil de conformidad	Descripción
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.
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.
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.
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.
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.

Gestión de perfiles de conformidad de BlackBerry Dynamics

Los perfiles de conformidad de BlackBerry Dynamics se importan desde Good Control cuando sincroniza Good Control con BlackBerry UEM. No puede editar los perfiles de conformidad de BlackBerry Dynamics, pero se pueden utilizar como referencia al crear nuevos perfiles de conformidad en BlackBerry 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 BlackBerry 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 BlackBerry UEM a los que se puede asignar también un usuario.

Configuración	Descripción
SO liberado	Esta configuración especifica las acciones que se producen cuando un usuario o un atacante evita diversas restricciones en un dispositivo para modificar el sistema operativo, instala aplicaciones no aprobadas u obtiene permisos elevados, y las acciones que se producen en las aplicaciones de BlackBerry Dynamics si se utiliza un sistema operativo liberado.

Configuración	Descripción
Verificación de la versión del SO	Esta configuración especifica las versiones del SO que están permitidas y restringidas, y las acciones que se producen en las aplicaciones de BlackBerry Dynamics si hay un SO restringido instalado en un dispositivo.
Verificación del modelo del hardware	Esta configuración especifica los modelos de hardware que están permitidos y restringidos, y las acciones que se producen en las aplicaciones de BlackBerry Dynamics si se usa un modelo de hardware restringido.
Verificación de versiones de bibliotecas de BlackBerry Dynamics	Esta configuración especifica las bibliotecas de BlackBerry Dynamics que se pueden usar y las acciones que se producen en las aplicaciones de BlackBerry Dynamics si el dispositivo utiliza una versión no permitida de la biblioteca.
Verificación de la conectividad	Esta configuración especifica si un dispositivo se debe conectar a BlackBerry UEM en un número especificado de días y las acciones que se producen en las aplicaciones de BlackBerry Dynamics si un dispositivo no se conecta a BlackBerry UEM. La configuración secundaria "Basar intervalo de conectividad en las aplicaciones delegadas de la autenticación" especifica si la aplicación configurada como la delegada de la autenticación gestiona el intervalo de conectividad. Si utiliza el delegado de autenticación para gestionar el intervalo de conectividad, las aplicaciones que se utilizan con menos frecuencia no se bloquearán ni eliminarán si no se conectan a BlackBerry UEM.

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 en la empresa, o si un dispositivo se pierde o se roba, puede enviar un comando para eliminar 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.

Enviar un comando a un dispositivo

Antes de empezar:

Si desea establecer un periodo de caducidad para los comandos que eliminan datos de los dispositivos con BlackBerry UEM, consulte Establecer un tiempo de caducidad para los comandos.

1. En la barra de menús, haga clic en **Usuarios > Dispositivos gestionados**.
2. Busque una cuenta de usuario.
3. En los resultados de la búsqueda, haga clic en el nombre de la cuenta de usuario.
4. Haga clic en la pestaña del dispositivo.
5. En la ventana **Gestionar dispositivo**, seleccione el comando que desee enviar al dispositivo.

Envío de un comando masivo

Puede enviar un comando a varias cuentas de usuario o dispositivos al mismo tiempo seleccionando los usuarios o dispositivos en la lista de usuarios y enviando un comando masivo.

Antes de empezar: Si desea establecer un periodo de caducidad para los comandos que eliminan datos de los dispositivos, consulte Establecer un tiempo de caducidad para comandos.

1. En la barra de menús, haga clic en **Usuarios > Dispositivos gestionados**.
2. Si fuera necesario, filtre la lista de usuarios.
3. Lleve a cabo una de las siguientes acciones:
   - Seleccione la casilla para marcar en la parte superior de la lista de usuarios para seleccionar todos los usuarios y dispositivos de la lista.
   - Seleccione la casilla para marcar correspondiente a los usuarios y dispositivos que desea incluir. Puede utilizar Mayús+clic para seleccionar varios usuarios.
4. En el menú, haga clic en uno de los siguientes iconos:

Icono	Descripción
	Buscar dispositivos Puede seleccionar un máximo de 100 dispositivos cada vez. Para obtener más información, consulte Ubicar un dispositivo.
	Enviar correo Para obtener más información, consulte Envío de un mensaje de correo electrónico a los usuarios.
	Enviar correo de activación Para obtener más información, consulte Envío de un mensaje de correo electrónico de activación a varios usuarios.
	Agregar a grupos de usuarios Puede seleccionar un máximo de 200 dispositivos cada vez. Para obtener más información, consulte Adición de usuarios a grupos de usuarios.
	Exportar Para obtener más información, consulte Exportación de la lista de usuarios a un archivo .csv.
	Eliminar dispositivos Para utilizar este comando masivo, debe ser un administrador de seguridad. Puede seleccionar un máximo de 200 dispositivos cada vez. Para obtener más información, consulte Referencia de comandos.
	Actualizar la información del dispositivo. Para obtener más información, consulte Referencia de comandos.
	Eliminar todos los datos del dispositivo Para utilizar este comando, debe ser un administrador de seguridad. Puede seleccionar un máximo de 200 dispositivos cada vez. Este comando masivo no es compatible con dispositivos macOS. Para obtener más información, consulte Referencia de comandos.
	Eliminar solo los datos de trabajo Para utilizar este comando, debe ser un administrador de seguridad. Puede seleccionar un máximo de 200 dispositivos cada vez. Para obtener más información, consulte Referencia de comandos.

Icono	Descripción
	Editar propiedad del dispositivo Puede seleccionar un máximo de 100 dispositivos cada vez. Para obtener más información, consulte Cambio de la etiqueta de propiedad del dispositivo.
	Actualizar SO Puede forzar los dispositivos con iOS supervisados para instalar una actualización del SO. Para utilizar este comando, debe ser un administrador de seguridad. Puede seleccionar un máximo de 200 dispositivos cada vez. Para obtener más información, consulte Actualización del SO en dispositivos de iOS supervisados.
	Cambiar contraseñas de la consola Puede enviar una contraseña de BlackBerry UEM Self-Service a varios usuarios al mismo tiempo. Para obtener más información, consulte Envío de una contraseña de BlackBerry UEM Self-Service a varios usuarios.

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 BlackBerry UEM, el comando permanece en estado pendiente y el dispositivo no se elimina de BlackBerry UEM a menos que se elimine manualmente. Opcionalmente, se puede configurar BlackBerry UEM para que elimine automáticamente los dispositivos cuando no se completan los mandos tras un tiempo especificado.

1. En la barra de menú, haga clic en **Configuración > Configuración general > Caducidad del comando Eliminar**.
2. Para una o ambas opciones **Eliminar todos los datos del dispositivo** y **Eliminar solo los datos de trabajo**, seleccione **Eliminar automáticamente el dispositivo si el comando no se ha completado**.
3. En el campo **Caducidad del comando**, indique tras cuántos días desea que caduque el comando y se elimine automáticamente el dispositivo de BlackBerry UEM.
4. Haga clic en **Guardar**.

Referencia de comandos

Los comandos que puede enviar a los dispositivos varían en función de los tipos de dispositivo y activación. Algunos comandos se pueden enviar a varios dispositivos a la vez.

Comandos para dispositivos con iOS

Estos comandos también se aplican a los dispositivos con 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 en el equipo. Para obtener más información, consulte Ver y guardar un informe de dispositivo.	Controles de MDM Privacidad del usuario
Ver acciones de dispositivo	Este comando muestra todas las acciones que están en curso en un dispositivo. Para obtener más información, consulte Ver acciones de 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 BlackBerry UEM una vez que lo elimine, solo se eliminarán los datos de trabajo del dispositivo. Para enviar este comando a varios dispositivos, consulte Envío de un comando masivo.	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 BlackBerry UEM cuando envía este comando, puede cancelar el comando o eliminar el dispositivo de la consola. Si el dispositivo se conecta a BlackBerry UEM una vez que lo elimine, se eliminarán los datos de trabajo del dispositivo. Para enviar este comando a varios dispositivos, consulte Envío de un comando masivo.	Controles de MDM Privacidad del usuario
Bloquear dispositivo	Este comando bloquea un dispositivo. El usuario debe escribir la contraseña del dispositivo para desbloquear el dispositivo. Si un dispositivo se pierde de manera temporal, puede utilizar este comando. 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

Comando	Descripción	Tipos de activación
Activar modo perdido	Este comando bloquea el dispositivo y le permite establecer un número de teléfono y un mensaje que se mostrará en el dispositivo. Por ejemplo, puede mostrar la información de contacto cuando se encuentre el dispositivo. Después de enviar este comando, podrá ver la ubicación del dispositivo desde BlackBerry UEM. 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 BlackBerry 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. Para obtener más información, consulte Actualización del sistema operativo en dispositivos iOS supervisados. Para enviar este comando a varios dispositivos, consulte Envío de un comando masivo. 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 a los dispositivos 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 a los dispositivos a desactivarse. Este comando solo es compatible con dispositivos supervisados. Este comando no es compatible con dispositivos Apple TV.	Controles de MDM
Limpiar aplicaciones	Este comando borra los datos de todas las aplicaciones gestionadas por Microsoft Intune en el dispositivo. Las aplicaciones no se eliminan del dispositivo. Para obtener más información, consulte Borrar aplicaciones gestionadas por Microsoft Intune.	Controles de MDM

Comando	Descripción	Tipos de activación
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. Para enviar este comando a varios dispositivos, consulte Envío de un comando masivo.	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 BlackBerry 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 BlackBerry UEM, el usuario recibe una notificación y el dispositivo no podrá comunicarse con BlackBerry UEM a menos que se reactive. Para enviar este comando a varios dispositivos, consulte Envío de un comando masivo.	Controles de MDM Privacidad del usuario
Actualización de planes móviles 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 con macOS

Comando	Descripción
Ver informe del dispositivo	Este comando muestra información detallada acerca de un dispositivo. Puede exportar y guardar el informe del dispositivo en el equipo. Para obtener más información, consulte Ver y guardar un informe de dispositivo.
Ver acciones de dispositivo	Este comando muestra todas las acciones que están en curso en un dispositivo. Para obtener más información, consulte Ver acciones de 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, aplicaciones y certificados que se encuentran en el dispositivo y, opcionalmente, elimina el dispositivo de BlackBerry UEM. Para enviar este comando a varios dispositivos, consulte Envío de un comando masivo.

Comando	Descripción
Eliminar todos los datos del dispositivo	Este comando elimina toda la información del usuario y los datos de aplicaciones del dispositivo. Restablece los ajustes predeterminados de fábrica del dispositivo, bloquea el dispositivo con el PIN que establezca y, opcionalmente, elimina el dispositivo de BlackBerry 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. Para enviar este comando a varios dispositivos, consulte Envío de un comando masivo.
Eliminar dispositivo	Este comando elimina el dispositivo de BlackBerry UEM. El dispositivo puede seguir recibiendo correos electrónicos y otros datos de trabajo. Para enviar este comando a varios dispositivos, consulte Envío de un comando masivo.

Comandos para dispositivos Android

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 en el equipo. Para obtener más información, consulte Ver y guardar un informe de dispositivo.	Todos (excepto BlackBerry 2FA)
Ver acciones de dispositivo	Este comando muestra todas las acciones que están en curso en un dispositivo. Para obtener más información, consulte Ver acciones de dispositivo.	Todos (excepto BlackBerry 2FA)
Bloquear dispositivo	Este comando bloquea el dispositivo. El usuario debe escribir la contraseña del dispositivo para desbloquear el dispositivo. Si un dispositivo se pierde de manera temporal, puede utilizar este comando. 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.	Controles de MDM Trabajo y personal: control total (Android Enterprise) Trabajo y personal: privacidad de usuario (Android Enterprise) Solo espacio de trabajo (Android Enterprise)

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 BlackBerry UEM cuando envía este comando, puede cancelar el comando o eliminar el dispositivo de la consola. Si el dispositivo se conecta a BlackBerry UEM una vez que lo elimine, solo se eliminarán los datos de trabajo del dispositivo, incluido el espacio de trabajo, si procede. Para enviar este comando a varios dispositivos, consulte Envío de un comando masivo.	Controles de MDM Trabajo y personal: control total (Android Enterprise) Trabajo y personal: control total (Samsung Knox) Solo espacio de trabajo - (Samsung Knox)
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, la información del espacio de trabajo y el espacio de trabajo se eliminarán del dispositivo, pero todas las aplicaciones y datos personales permanecerán en el dispositivo. Para obtener más información, consulte Desactivación de dispositivos. 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. Para activaciones Trabajo y personal: control total (Android Enterprise), este comando solo es compatible con dispositivos que ejecuten Android 11 y posterior. 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 BlackBerry UEM una vez que lo haya eliminado, se eliminarán los datos de trabajo del dispositivo, incluido el espacio de trabajo, si procede. Para enviar este comando a varios dispositivos, consulte Envío de un comando masivo.	Controles de MDM Trabajo y personal: privacidad de usuario (Android Enterprise) Trabajo y personal: control total (Android Enterprise) Trabajo y personal: privacidad de usuario (Samsung Knox) Trabajo y personal: control total (Samsung Knox) Solo espacio de trabajo - (Samsung Knox)
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. **Nota:** Este comando no es compatible con dispositivos con Samsung Knox SDK 3.2.1 y posterior.	Controles de MDM (solo dispositivos Samsung) Trabajo y personal: control total (Samsung Knox) Trabajo y personal: privacidad de usuario (Samsung Knox)

Comando	Descripción	Tipos de activación
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. **Nota:** Para los tipos de activación Trabajo y personal: privacidad de usuario, solo los dispositivos BlackBerry con Android 8.x y posteriores son compatibles con este comando. **Nota:** Para el tipo de activación Trabajo y personal: control total (Android Enterprise), solo los dispositivos que utilizan una versión del sistema operativo Android anterior a Android 11 admiten este comando.	Trabajo y personal: control total (Samsung Knox) Solo espacio de trabajo (Android Enterprise) Trabajo y personal: control total (Android Enterprise) Trabajo y personal: privacidad de usuario (Android Enterprise)
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) Solo espacio de trabajo - (Samsung Knox)
Especificar contraseña de espacio de trabajo y bloquear	Puede 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: privacidad de usuario (Android Enterprise) Trabajo y personal: control total (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 (Samsung Knox) Trabajo y personal: privacidad de usuario - (Samsung Knox) Solo espacio de trabajo - (Samsung Knox)
Desactivar BlackBerry 2FA	Este comando desactiva los dispositivos que se activan con el tipo de activación BlackBerry 2FA. El dispositivo se elimina de BlackBerry 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 por Microsoft Intune en el dispositivo. Las aplicaciones no se eliminan del dispositivo. Para obtener más información, consulte Borrar aplicaciones gestionadas por Microsoft Intune.	Todas (excepto BlackBerry 2FA)

Comando	Descripción	Tipos de activación
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. Para enviar este comando a varios dispositivos, consulte Envío de un comando masivo.	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 Enterprise)
Eliminar dispositivo	Este comando elimina el dispositivo de BlackBerry 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 BlackBerry UEM, el usuario recibe una notificación y el dispositivo no podrá comunicarse con BlackBerry UEM a menos que se reactive. Para enviar este comando a varios dispositivos, consulte Envío de un comando masivo.	Todos (excepto BlackBerry 2FA)

Comandos para dispositivos con Windows

Comando	Descripción
Ver informe del dispositivo	Este comando muestra información detallada acerca de un dispositivo. Puede exportar y guardar el informe del dispositivo en el equipo. Para obtener más información, consulte Ver y guardar un informe de dispositivo.
Ver acciones de dispositivo	Este comando muestra todas las acciones que están en curso en un dispositivo. Para obtener más información, consulte Ver acciones de dispositivo.

Comando	Descripción
Bloquear dispositivo	Este comando bloquea un dispositivo. El usuario debe escribir la contraseña del dispositivo para desbloquear el dispositivo. Si un dispositivo se pierde de manera temporal, puede utilizar este comando. 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, aplicaciones y 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 BlackBerry UEM. Si el dispositivo no se puede conectar a BlackBerry UEM, puede eliminar el dispositivo de BlackBerry UEM. Si el dispositivo se conecta a BlackBerry UEM una vez que lo haya eliminado, solo se eliminarán los datos de trabajo del dispositivo, incluido el espacio de trabajo, si procede. Para enviar este comando a varios dispositivos, consulte Envío de un comando masivo.
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, elimina el dispositivo de BlackBerry UEM. Después de enviar este comando, se le dará la opción de eliminar el dispositivo de BlackBerry UEM. Si el dispositivo no se puede conectar a BlackBerry UEM, puede eliminar el dispositivo de BlackBerry UEM. Si el dispositivo se conecta a BlackBerry UEM una vez que lo haya eliminado, solo se eliminarán los datos de trabajo del dispositivo, incluido el espacio de trabajo, si procede. Para enviar este comando a varios dispositivos, consulte Envío de un comando masivo.
Reinicie el escritorio o dispositivo	Este comando fuerza a los dispositivos a reiniciarse.

Comando	Descripción
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. 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. Para enviar este comando a varios dispositivos, consulte Envío de un comando masivo.
Eliminar dispositivo	Este comando elimina el dispositivo de BlackBerry UEM. El dispositivo puede seguir recibiendo correos electrónicos y otros datos de trabajo. Para enviar este comando a varios dispositivos, consulte Envío de un comando masivo.

Desactivación de dispositivos

Cuando usted o un usuario desactiva el dispositivo, la conexión entre el dispositivo y la cuenta de usuario en BlackBerry UEM se elimina. No se puede gestionar el dispositivo y ya no aparece en la consola de gestión. El usuario no puede acceder a los datos de trabajo en el dispositivo.

Puede desactivar un dispositivo mediante el comando "Eliminar solo los datos de trabajo" o "Eliminar todos los datos del dispositivo". BlackBerry UEM también puede desactivar un dispositivo si este infringe el perfil de cumplimiento y la acción de cumplimiento es desactivar el dispositivo. Los usuarios pueden desactivar los dispositivos a través de los siguientes métodos:

- Para los dispositivos con iOS y Android, los usuarios pueden seleccionar Desactivar mi dispositivo en la pantalla Acerca de en la aplicación BlackBerry UEM Client.
- Para los dispositivos Windows 10, los usuarios pueden seleccionar Configuración > Cuentas > Acceso de trabajo > Eliminar.

Para los dispositivos que usan Knox MDM, cuando el dispositivo está desactivado, se desinstalan las aplicaciones internas y la opción de desinstalación está disponible para cualquier aplicación pública que se haya instalado desde la lista de aplicaciones según sea necesario.

Para los dispositivos con Android Enterprise que solo tengan un perfil de trabajo, si desactiva un dispositivo, puede eliminar todos los datos de la tarjeta SD y eliminar la protección de restablecimiento de fábrica.

Para los dispositivos con Android Enterprise con activaciones Trabajo y personal: privacidad de usuario y Trabajo y personal: control total, si utiliza el comando "Eliminar solo los datos de trabajo", puede escribir un motivo que explique por qué se ha borrado el perfil de trabajo para que aparezca en la notificación del dispositivo del usuario. Si el dispositivo se desactiva por infringir las normas de cumplimiento, la notificación especifica el motivo por el cual el dispositivo no cumplía con los requisitos de cumplimiento.

Para dispositivos Android Enterprise con activaciones Trabajo y personal: control total, solo el comando "Eliminar todos los datos del dispositivo" es compatible con dispositivos que ejecuten Android 10 y anteriores. El comando "Eliminar solo los datos de trabajo" es compatible con dispositivos que ejecutan Android 11 y versiones posteriores. El comando "Eliminar solo los datos de trabajo" elimina todos los datos de trabajo y aplicaciones, pero permite al usuario conservar los datos personales y las aplicaciones, y seguir utilizando el dispositivo no gestionado.

En los dispositivos Samsung Knox Workspace que se han activado mediante los tipos de activación Trabajo y personal: control total o Solo espacio de trabajo, al desactivar el dispositivo se eliminan todos los datos del dispositivo o solo del espacio de trabajo. Puede especificar los datos que se borran utilizando la regla de política de TI "Borrado de datos durante la desactivación".

Control de las actualizaciones de software instaladas en los dispositivos

Puede controlar las versiones de software del dispositivo instaladas en dispositivos con Android Enterprise y Samsung Knox. Para dispositivos Android Enterprise, también puede configurar un periodo de actualización para aplicaciones que se ejecuten en primer plano.

Para dispositivos Android Enterprise con activaciones de Solo espacio de trabajo y Trabajo y personal: control total, puede especificar si el usuario puede elegir cuándo instalar actualizaciones de software disponibles o si estas actualizaciones se instalarán automáticamente. Puede especificar reglas diferentes en función del modelo de dispositivo y la versión del sistema operativo instalada actualmente. Para todos los dispositivos Android Enterprise, también puede configurar un periodo de actualización para acceder a las aplicaciones que se ejecutan en el primer plano porque, de forma predeterminada, cuando una aplicación se ejecuta en primer plano, Google Play no se puede actualizar. También puede controlar cómo Google Play aplica los cambios en el dispositivo, por ejemplo, especificando si el usuario puede permitir el cambio o si el cambio se produce cuando el dispositivo está conectado a una red Wi-Fi.

En dispositivos Android Enterprise con activaciones de Solo espacio de trabajo y Trabajo y personal: control total, para cualquier dispositivo para el cual haya especificado una regla de actualización del SO diferente de la predeterminada, también puede suspender las actualizaciones durante las fechas en las que no es pertinente efectuar actualizaciones. Por ejemplo, puede que desee suspender las actualizaciones durante los periodos de vacaciones. Si desea suspender las actualizaciones para todos los dispositivos, primero debe crear una regla de actualización del SO para todos los dispositivos. Por ejemplo, puede crear una regla de actualización del SO para todos los dispositivos que ejecuten Android 7.0 y versiones posteriores a fin de aplicar actualizaciones automáticamente a determinadas horas.

En dispositivos con Samsung Knox, puede utilizar Enterprise Firmware Over the Air (E-FOTA) para controlar cuándo se instalan las actualizaciones de firmware de Samsung.

Nota: Samsung E-FOTA llegará al final de su ciclo de servicio el 31 de julio de 2022. Para obtener más información, consulte la información de Samsung. Para obtener información sobre la migración a Samsung E-FOTA One, visite support.blackberry.com y lea el artículo 69901.

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

E-FOTA 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).

El control de las versiones garantiza que los dispositivos de los usuarios utilizan las versiones de firmware compatibles con sus aplicaciones y cumplen las políticas de su empresa. Puede utilizar un perfil de Requisitos de solicitud de servicio del dispositivo para crear reglas de firmware para los dispositivos Samsung Knox activados en UEM. Puede programar cuándo se instalan las actualizaciones de firmware y especificar cuándo se deben instalar actualizaciones forzosas. Para obtener más información sobre E-FOTA, visite https://seap.samsung.com/sdk/enterprise-fota.

Nota: En función del proveedor de servicios inalámbricos que utilice un dispositivo, es posible que las actualizaciones de E-FOTA no estén disponibles. Algunos proveedores de servicios inalámbricos (por ejemplo, AT&T y Verizon) utilizan sus propios sistemas para administrar las actualizaciones inalámbricas.

En dispositivos con activaciones de Controles de MDM, no puede controlar el momento y la forma en la que los usuarios actualizan el SO de sus dispositivos, pero puede utilizar perfiles de conformidad para restringir la versión del SO del equipo. Para ejecutar una acción determinada si la versión de software restringida se instala en un dispositivo, debe crear un perfil de conformidad y asignarlo a los usuarios, los grupos de usuarios o los grupos de

dispositivos. Esta acción es válida para todos los dispositivos. El perfil de cumplimiento especifica las acciones que se llevan a cabo si el usuario no elimina la versión de software restringida del dispositivo.

No puede controlar las versiones de software instaladas en dispositivos con iOS, pero puede forzar a los dispositivos con iOS supervisados a instalar una actualización disponible. Para obtener más información, consulte Actualización del SO en dispositivos de iOS supervisados.

Crear un perfil de requisitos de solicitud de servicio del dispositivo para dispositivos con Android Enterprise

Las reglas de actualización del SO se aplican únicamente a dispositivos Solo espacio de trabajo y Trabajo y personal: control total. Estas reglas se aplican a todos los dispositivos Android Enterprise. Para obtener más información sobre las reglas de configuración de los dispositivos Samsung Knox que utilizan E-FOTA, consulte Crear un perfil de requisitos de solicitud de servicio del dispositivo para dispositivos con Samsung Knox.

Nota: Samsung E-FOTA llegará al final de su ciclo de servicio el 31 de julio de 2022. Para obtener más información, consulte la información de Samsung. Para obtener información sobre la migración a Samsung E-FOTA One, visite support.blackberry.com y lea el artículo 69901.

1. En la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Conformidad > Requisitos de solicitud de servicio del dispositivo**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil.
5. Haga clic en la pestaña **Android**.
6. Para los dispositivos Solo espacio de trabajo y Trabajo y personal: control total, siga los siguientes pasos para establecer las reglas para la actualización del SO:
   a) En la tabla **Regla de actualización del SO**, haga clic en el +.
   b) En la lista desplegable **Modelo de dispositivo**, seleccione un modelo de dispositivo.
   c) En la lista desplegable **Versión del SO**, seleccione la versión del sistema operativo.
   d) En la lista desplegable **Regla de actualización**, seleccione una de las siguientes opciones:
      - Seleccione **Predeterminado** para permitir que el usuario elija cuánto instalar las actualizaciones.
      - Seleccione **Actualizar automáticamente** para instalar las actualizaciones sin preguntar al usuario.
      - Seleccione **Actualizar automáticamente entre** para instalar las actualizaciones entre las horas especificadas sin preguntar al usuario. El usuario puede elegir que las actualizaciones se instalen fuera de este intervalo.
      - Seleccione **Retrasar hasta 30 días** para 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.
   e) Cuando haya terminado, haga clic en **Agregar**.
   f) Repita los el paso 6 para cada regla que desee agregar.

   Las reglas establecidas para los dispositivos con Samsung Knox que utilizan E-FOTA tienen prioridad sobre estas reglas.
7. Si desea especificar periodos en los que no se pueden realizar actualizaciones del SO en los dispositivos con Solo espacio de trabajo y Trabajo y personal: control total, proceda como se indica a continuación:
   a) En la tabla **Suspender actualizaciones del SO**, haga clic en el +.
   b) En la lista desplegable **Mes de inicio**, seleccione el mes en el que comenzará el periodo de suspensión.
   c) En la lista desplegable **Día de inicio**, seleccione el día en el que comenzará el periodo de suspensión.

d) En la lista desplegable **Duración**, seleccione el periodo de tiempo de la suspensión.

La suspensión no puede superar los 90 días. Si especifica más de un periodo de suspensión, debe haber al menos 60 días entre los periodos.

Estas configuraciones no se aplican a los dispositivos con Samsung Knox que utilizan E-FOTA.

8. Para especificar un periodo de actualización para las aplicaciones que se ejecutan en el primer plano, seleccione la opción **Activar el periodo de actualización para aplicaciones que se ejecutan en primer plano** y establezca las siguientes opciones:
   - **Hora de inicio (hora local del dispositivo)**: especifica la hora en que comenzará a actualizarse la aplicación.
   - **Duración**: especifica el número de horas que permitirá que se actualicen las aplicaciones.
9. Para especificar el modo en que Google Play aplica los cambios a las aplicaciones que se ejecutan en el primer plano, seleccione Política de actualización automática de aplicaciones. Seleccione una de las siguientes opciones:
   - **El usuario puede permitir**: se le pedirá al usuario que permita que se actualicen aplicaciones en el dispositivo. Tenga en cuenta que esta será la configuración predeterminada si no cancela la selección de la opción Política de actualización automática de aplicaciones.
   - **Siempre**: las aplicaciones se actualizarán siempre. Tenga en cuenta que para una aplicación que se esté ejecutando siempre, como BlackBerry UEM Client, BlackBerry Work o BlackBerry Connectivity, si no selecciona **Activar el periodo de actualización para aplicaciones que se ejecutan en primer plano**, la aplicación no se actualizará hasta que el usuario la actualice manualmente en el dispositivo.
   - **Solo Wi-Fi**: las aplicaciones se actualizarán solamente cuando el dispositivo está conectado a una red Wi-Fi. Tenga en cuenta que para una aplicación que se esté ejecutando siempre, como BlackBerry UEM Client, BlackBerry Work o BlackBerry Connectivity, si no selecciona **Activar el periodo de actualización para aplicaciones que se ejecutan en primer plano**, la aplicación no se actualizará hasta que el usuario la actualice manualmente en el dispositivo.
   - **Desactivar**: las aplicaciones nunca se actualizarán.

     Nota:

     Este perfil afecta a la configuración de las aplicaciones de actualización automática de Google Play. Si selecciona **Siempre**, **Solo Wi-Fi** o **Desactivar**, el usuario no podrá seleccionar una opción diferente en el dispositivo. Por ejemplo, si selecciona **Desactivar** en el perfil, el usuario no podrá activar las actualizaciones de una aplicación en el dispositivo. Sin embargo, los usuarios podrán seguir actualizando manualmente las aplicaciones en Google Play.
10. Haga clic en **Agregar**.

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

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

Nota: En función del proveedor de servicios inalámbricos que utilice un dispositivo, es posible que las actualizaciones de E-FOTA no estén disponibles. Algunos proveedores de servicios inalámbricos (por ejemplo, T&T y Verizon) utilizan sus propios sistemas para administrar las actualizaciones inalámbricas.

Antes de empezar: Compruebe que se ha agregado una licencia de E-FOTA a BlackBerry UEM. Para utilizar E-FOTA, debe seleccionar la regla para permitir las actualizaciones OTA global de Android en la política de TI asociada en la consola de administración de BlackBerry UEM.

Nota: Samsung E-FOTA llegará al final de su ciclo de servicio el 31 de julio de 2022. Para obtener más información, consulte la información de Samsung. Para obtener información sobre la migración a Samsung E-FOTA One, visite support.blackberry.com y lea el artículo 69901.

1. En la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Conformidad > Requisitos de solicitud de servicio del dispositivo**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil.
5. En la tabla **Reglas de firmware del dispositivo Samsung**, haga clic en +.
6. Seleccione **Aplicar restricción a todos los dispositivos Android** para permitir Android OS que se apliquen las actualizaciones a Samsung los dispositivos.
7. En el campo **Modelo de dispositivo**, introduzca el modelo de dispositivo o seleccione uno en la lista desplegable.
8. En la lista desplegable **Idioma**, seleccione un idioma.
9. En el campo **Código del operador**, introduzca el código CSC del proveedor de servicios inalámbricos para el dispositivo.
10. Haga clic en **Obtener versión de firmware**.
11. Repita los pasos del 5 al 8 para cada regla de firmware que desee agregar.
12. Cuando haya terminado, haga clic en **Agregar**.
13. En la tabla **Reglas de firmware del dispositivo Samsung**, haga clic en **Horario** junto a la versión de firmware que ha agregado.
14. En el cuadro de diálogo **Programar actualización forzada**, haga lo siguiente: (**Nota**: Si selecciona la opción Programar actualización forzada, el dispositivo Knox ya no estará restringido a la versión de firmware y podrá actualizarlo manualmente si hay disponible una versión posterior):
    a) En los campos **Programar actualización forzada entre**, seleccione el intervalo de fechas en el que se debe instalar la actualización. El intervalo de fechas debe estar entre 3 y 7 días. El valor predeterminado es 7 días.
    b) En las listas desplegables **Programar actualización forzada durante las horas de**, especifique cuándo se debe instalar la actualización forzada y la zona horaria del usuario. El intervalo de tiempo debe estar entre 1 y 12 horas.
15. Haga clic en **Guardar**.

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

Añadir una licencia de E-FOTA

Puede utilizar Enterprise Firmware Over the Air (E-FOTA) para controlar cuándo se instalan las actualizaciones de firmware de Samsung en los dispositivos Samsung Knox. El control de las versiones garantiza que los dispositivos de los usuarios utilizan las versiones de firmware compatibles con sus aplicaciones y cumplen las políticas de su empresa.

Antes de crear un perfil de requisitos de versión de software del dispositivo para controlar las versiones de firmware, debe agregar una licencia de E-FOTA en UEM.

Nota: Samsung E-FOTA llegará al final de su ciclo de servicio el 31 de julio de 2022. Para obtener más información, consulte la información de Samsung. Para obtener información sobre la migración a Samsung E-FOTA One, visite support.blackberry.com y lea el artículo 69901.

1. En la barra de menú, haga clic en **Licencias** > **Resumen de licencias**.
2. En la sección **E-FOTA**, haga clic en **Añadir licencia**.

3. En el cuadro de diálogo **Añadir una licencia de E-FOTA**, introduzca el nombre, el ID de cliente, el secreto de cliente, el ID de cliente y la clave de licencia.
4. Haga clic en **Guardar**.

Presentación de los usuarios que están ejecutando una versión de software rechazada

Puede ver una lista de los usuarios que están ejecutando una versión de software rechazada. Una versión de software rechazada es una versión de software que un proveedor de servicios ya no acepta, pero que aún se puede instalar en el dispositivo del usuario.

1. En la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Conformidad > Requisitos de solicitud de servicio del dispositivo**.
3. Haga clic en el nombre del perfil que desea consultar.
4. Haga clic en la pestaña **x usuarios con solicitud de servicio rechazada** para ver la lista de usuarios que están ejecutando una versión de software rechazada.

Gestión de actualizaciones del sistema operativo en dispositivos con activaciones de Controles de MDM

No puede controlar el momento en el que se instalan versiones de software en dispositivos con activaciones de Controles de MDM. Sin embargo, puede utilizar perfiles de conformidad para ayudarle a gestionar los dispositivos que los usuarios han actualizado a una versión del sistema operativo que no permite su empresa. Por ejemplo, los dispositivos con Android 10 y versiones posteriores no son compatibles con las activaciones de Controles de MDM. Si los usuarios con dispositivos que ejecutan Android 9.x actualizan a Android 10, algunas funciones de gestión dejarán de funcionar, por lo que el dispositivo estará en riesgo. Puede utilizar grupos de dispositivos y perfiles de conformidad para detectar los dispositivos con Android con el tipo de activación Controles de MDM y establecer reglas de conformidad para tomar las medidas pertinentes, como notificar al usuario, no confiar en el dispositivo o dejar de gestionar el dispositivo.

Siga estos pasos para gestionar las actualizaciones del sistema operativo en los dispositivos con activaciones Controles de MDM.

Paso	Acción
1	Crear un grupo de dispositivos que incluya dispositivos que cumplan los siguientes requisitos: • Tipo de activación de Controles de MDM • Versión del sistema operativo del dispositivo que desee restringir Si un usuario actualiza un dispositivo al sistema operativo especificado, automáticamente pasa a formar parte del grupo de dispositivos.
2	Crear un perfil de conformidad y especificar la versión del sistema operativo del dispositivo como versión restringida del sistema operativo.

Paso	Acción
3	En el perfil de conformidad, especifique la acción de cumplimiento adecuada para su empresa. Por ejemplo, puede indicar al usuario que su tipo de activación no es compatible con el sistema operativo del dispositivo y recomendarle que vuelva a activar el dispositivo con un tipo de activación diferente, o puede desactivar el dispositivo.
4	Asignar el perfil de conformidad al grupo de dispositivos.
5	De forma opcional, cree una notificación de evento para informar a los administradores cuando un dispositivo no cumpla los requisitos del perfil de conformidad.

Vea las actualizaciones disponibles para dispositivos iOS

Puede ver si hay una actualización de software disponible para los dispositivos iOS de sus usuarios, de forma que puedan actualizar el software a la versión más reciente.

1. En la barra de menú, haga clic en **Usuarios > Dispositivos gestionados**.
2. Busque una cuenta de usuario.
3. En los resultados de la búsqueda, haga clic en el nombre de la cuenta de usuario.
4. Seleccione la pestaña dispositivo.
5. En la sección de dispositivo Activado, consulte si hay una actualización disponible.

Actualización del SO en dispositivos de iOS supervisados

Puede forzar los dispositivos iOS para instalar una actualización del SO. Para actualizar el SO en varios dispositivos, consulte Envío de un comando masivo.

También puede controlar la fecha de las actualizaciones de software de iOS mediante las reglas de políticas de TI "Retrasar actualizaciones de software" y "Periodo de retraso de actualizaciones de software" Para obtener más información, descargue la hoja de cálculo de referencia de políticas.

1. En la barra de menú, haga clic en **Usuarios > Dispositivos gestionados**.
2. Busque una cuenta de usuario.
3. En los resultados de la búsqueda, haga clic en el nombre de la cuenta de usuario.
4. Haga clic en la pestaña del dispositivo.
5. En el panel izquierdo, si hay una actualización de software disponible, haga clic en **Actualizar ahora**.
6. En la lista desplegable, seleccione una de las opciones siguientes:
   - **Descargar e instalar**: la actualización se descarga e instala automáticamente en el dispositivo.
   - **Solo descarga**: la actualización se descarga automáticamente en el dispositivo y se le solicita al usuario que la instale.
   - **Instalar las actualizaciones descargadas**: si la actualización ya se ha descargado en un dispositivo, se instala automáticamente.
7. En la lista **Versión de SO**, seleccione la versión con la que desea actualizar el dispositivo.
8. Haga clic en **Actualizar**.

Configuración de la comunicación entre los dispositivos y BlackBerry UEM

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, BlackBerry UEM solicita al dispositivo que se ponga en contacto con BlackBerry UEM para recibir actualizaciones. Si por algún motivo el dispositivo no recibe el aviso, el perfil de Enterprise Management Agent se utiliza para asegurarse de que el dispositivo se pone en contacto con BlackBerry UEM en los intervalos que especifique.

En entornos locales, también puede utilizar el perfil Enterprise Management Agent para permitir que BlackBerry UEM pueda recopilar una lista de aplicaciones personales en los dispositivos de los usuarios. Para desactivar la recopilación de aplicaciones personales, debe desmarcar la opción "Permitir recopilaciones de aplicaciones personales". Para obtener más información, consulte Desactivación de la recopilación de aplicaciones personales.

Se puede asignar un perfil de Enterprise Management Agent a usuarios, a grupos de usuarios y a grupos de dispositivos.

Creación de un perfil de Enterprise Management Agent

1. En la barra de menú, haga clic en **Políticas y perfiles**.
2. Haga clic en **Política > Enterprise Management Agent**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil.
5. Establezca los valores para cada tipo de dispositivo que requiera la empresa.
6. Haga clic en **Agregar**.

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

iOS: configuración del perfil de Enterprise Management Agent

Configuración	Descripción
Frecuencia de sondeo de Enterprise Management Agent	Especifique con qué frecuencia, en segundos, desea que el dispositivo busque comandos de servidor de Enterprise Management Agent. El dispositivo solo realiza búsquedas cuando UEM Client está abierta en el dispositivo. Valores posibles: • De 900 a 86400 El valor predeterminado es 3600.
Permitir colecciones de aplicaciones personales	Esta opción especifica si desea que BlackBerry UEM reciba una lista de las aplicaciones personales que están instaladas en los dispositivos de los usuarios. 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. Valores posibles: • De 3600 a 86400 segundos El valor predeterminado es 3600.
Umbral del nivel de batería	Especifique el cambio en el porcentaje de nivel de batería (de 5 a 100) obligatorio antes de que el dispositivo envíe la información de nuevo a BlackBerry UEM. Valores posibles: • Del 5 al 100 por ciento El valor predeterminado es 20.
Umbral de espacio libre de RAM	Especifique el cambio requerido en la cantidad de memoria libre en megabytes antes de que el dispositivo envíe la información de nuevo a BlackBerry UEM. De manera predeterminada, el dispositivo no envía esta información de nuevo a BlackBerry 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 BlackBerry UEM. El valor predeterminado es 250.
Umbral de la tarjeta de memoria	Especifique el cambio requerido en la cantidad de espacio externo libre en megabytes antes de que el dispositivo envíe la información de nuevo a BlackBerry UEM. El valor predeterminado es 500.
Frecuencia de sondeo de Enterprise Management Agent	Especifique con qué frecuencia, en segundos, desea que el dispositivo busque comandos de servidor de Enterprise Management Agent. Valores posibles: • Mínimo: 900 El valor predeterminado es 900.
Permitir colecciones de aplicaciones personales	Esta opción especifica si desea que BlackBerry UEM reciba una lista de las aplicaciones personales que están instaladas en los dispositivos de los usuarios. 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.
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	Esta opción especifica si desea que BlackBerry UEM reciba una lista de las aplicaciones personales que están instaladas en los dispositivos de los usuarios.

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 con iOS, macOS, Android y Windows 10, puede crear avisos de empresa personalizados para que se muestren durante la activación. Por ejemplo, un aviso puede contener las condiciones que un usuario debe seguir 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 para cubrir diferentes requisitos y puede crear versiones separadas de cada aviso para que sean compatibles con idiomas diferentes.

Puede crear perfiles de dispositivo para mostrar información sobre la empresa en los dispositivos. En dispositivos con iOS y Android, la información de la empresa se muestra en BlackBerry UEM Client en el dispositivo. 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.

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

Dónde se muestra la información de la empresa	Cómo configurar la información de la empresa
Mostrar un aviso de la empresa al realizar la activación en los dispositivos con iOS, macOS, Android y Windows 10	Cree un aviso de la empresa y asígnelo a un perfil de activación.
Mostrar un aviso de la empresa al reiniciar en los dispositivos Samsung Knox	Cree un aviso de la empresa y asígnelo en la pestaña Android del perfil de dispositivo. Para cambiar el aviso que aparece al reiniciar el dispositivo, debe actualizar el perfil de dispositivo.
Mostrar la información de la empresa en los dispositivos con BlackBerry UEM Client en iOS y Android, o en la información de soporte técnico en los dispositivos con Windows 10.	Escriba la información que quiere que se muestre en la pestaña correspondiente del perfiles de dispositivo.
En una imagen de fondo de pantalla en los dispositivos con Samsung Knox o iOS supervisados	Seleccione un archivo de imagen en la pestaña correspondiente del perfiles de dispositivo.

Crear avisos de la empresa

Puede crear avisos de empresa personalizados para que se muestren durante la activación de los dispositivos con iOS, macOS, Android y Windows 10.

Los dispositivos con Samsung Knox también pueden mostrar el aviso de la empresa cuando un usuario los reinicia.

1. En la barra de menús, haga clic en **Configuración**.
2. En el panel izquierdo, amplíe **Configuración general**.
3. Haga clic en **Avisos de la empresa**.
4. Haga clic en + en el lateral derecho de la pantalla.
5. En el campo **Nombre**, escriba un nombre para el aviso de la empresa.
6. 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**.
7. En la lista desplegable **Idioma del dispositivo**, seleccione el idioma que desea utilizar como idioma predeterminado para el aviso de la empresa.
8. En el campo **Aviso de la empresa**, escriba el texto del aviso de la empresa.
9. Opcionalmente, puede hacer clic varias veces en **Agregar un idioma adicional** para publicar el aviso de la empresa en más idiomas.
10. 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.
11. 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: En los dispositivos con Samsung Knox, cree avisos de la empresa.

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

1. En la barra de menús, haga clic en **Políticas y perfiles**.
2. Haga clic en **Personalizada > Dispositivo**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil. Cada perfil de dispositivo debe tener un nombre único.
5. Lleve a cabo una de las tareas siguientes:

Tarea	Pasos
Asignación de un aviso de la empresa para que se muestre en los dispositivos con Samsung Knox mientras se reinician	**a.** Haga clic en **BlackBerry** o **Android**. **b.** En la lista desplegable **Asignar aviso de la organización**, seleccione el aviso de la empresa que desea que se muestre en los dispositivos.
En los dispositivos con 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.	**a.** Haga clic en **iOS**, **Android** o **Windows**. **b.** Escriba el nombre, dirección, número de teléfono y dirección de correo de la empresa.

6. Si fuera necesario, realice las tareas siguientes:

Tarea	Pasos
Adición de una imagen de fondo de pantalla al espacio de trabajo de los dispositivos con Samsung Knox	**a.** Haga clic en **BlackBerry** o **Android**. **b.** En la sección **Fondo de pantalla del espacio de trabajo**, haga clic en **Examinar**. **c.** Seleccione la imagen que desea utilizar como fondo de pantalla. **d.** Haga clic en **Abrir**.
Añadir una imagen de fondo de pantalla a los dispositivos iOS supervisados	**a.** Haga clic en **iOS**. **b.** En la sección **Fondo de pantalla del dispositivo**, seleccione si el fondo de pantalla debe mostrarse en la **Pantalla de inicio**, la **Pantalla de bloqueo** o **Ambas**. **c.** Haga clic en **Examinar** y seleccione la imagen que desea utilizar como fondo de pantalla. **d.** Haga clic en **Abrir**. **e.** En el campo **Configurar el fondo de pantalla para**, seleccione el lugar donde desea que se muestre el fondo de pantalla.

7. Haga clic en **Agregar**.

Después de terminar:

- Si fuera necesario, clasifique los perfiles.

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 autorizar a los usuarios a localizar 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 los administradores pueden 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 móvil, de GPS y redes Wi-Fi para determinar la ubicación del dispositivo.

Configurar las opciones del servicio de ubicación

Puede configurar las opciones de los perfiles de servicio de ubicación, como la unidad de velocidad que se muestra en un dispositivo al ver su ubicación en un mapa. Si habilita el historial de ubicaciones en los dispositivos con iOS y Android, BlackBerry UEM almacena el historial de ubicaciones durante un mes de manera predeterminada.

1. En la barra de menú, haga clic en **Configuración > Configuración general > Servicio de ubicación**.
2. Si tiene un entorno local, en el campo **Antigüedad del historial de ubicación**, especifique el número de días, semanas o meses que BlackBerry UEM debe guardar el historial de ubicaciones de los dispositivos.
3. En la lista desplegable **Unidad de velocidad mostrada** haga clic en **km/h** o **mph**.
4. Haga clic en **Guardar**.

Creación de un perfil de servicio de ubicación

Puede asignar un perfil del servicio de ubicación a cuentas de usuario, grupos de usuarios o grupos de dispositivos. Los usuarios deben aceptar el perfil con anterioridad para que la consola de administración o BlackBerry UEM Self-Service puedan mostrar las ubicaciones de los dispositivos con iOS y Android en un mapa. Los dispositivos con Windows 10 Mobile aceptan automáticamente el perfil.

Antes de empezar: Configurar las opciones del servicio de ubicación

1. En la barra de menú, haga clic en **Políticas y perfiles**.
2. Haga clic en **Protección > Servicio de ubicación**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil de servicio de ubicación.
5. Opcionalmente, desactive la casilla de verificación para cualquier tipo de dispositivo para el que no desee configurar el perfil.
6. Lleve a cabo cualquiera de las tareas siguientes:

Tarea	Pasos
Activar el historial de ubicaciones en dispositivos con iOS	**a.** En la pestaña **iOS**, compruebe que la casilla de verificación **Registrar historial de ubicaciones de dispositivo** está seleccionada. **Nota:** 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 con Android	**a.** En la pestaña **Android**, compruebe que la casilla de verificación **Registrar historial de ubicaciones de dispositivo** está seleccionada. **b.** En el campo **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 el campo **Frecuencia de actualización de la ubicación**, especifique con qué frecuencia se actualiza la ubicación del dispositivo. **Nota:** Se deben cumplir las condiciones de distancia y frecuencia antes de que se actualice la ubicación del dispositivo.

7. Haga clic en **Agregar**.

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

Ubicar un dispositivo

Puede localizar dispositivos con iOS, Android y Windows 10 Mobile (por ejemplo, si se extravía o se roba un dispositivo). Los usuarios deben aceptar el perfil de servicio de ubicación con anterioridad para que la consola de administración muestre las ubicaciones de los dispositivos con iOS y Android en un mapa. Los dispositivos con Windows 10 Mobile aceptan automáticamente el perfil. El historial de ubicaciones está disponible para dispositivos con iOS y Android si los ha activado en el perfil.

Antes de empezar: Cree y asigne un perfil de servicio de ubicación.

1. En la barra de menú, haga clic en **Usuarios > Dispositivos gestionados**.
2. Seleccione la casilla de verificación correspondiente a los dispositivos que desea ubicar.
3. Haga clic en .
4. Encuentre los dispositivos en el mapa con los siguientes iconos. Si un dispositivo con 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.
   - Ubicación actual: 
   - Última ubicación conocida: 

   Puede hacer clic o desplazar el cursor sobre un icono para mostrar la información de ubicación, como latitud y longitud, y cuándo se informó de la ubicación (por ejemplo, hace un minuto o hace dos horas).
5. Para ver el historial de ubicaciones de un dispositivo con iOS o Android, realice las siguientes acciones:
   a) Haga clic en **Ver historial de ubicaciones**.
   b) Seleccione un intervalo de fecha u hora.

c) Haga clic en **Enviar**.

Uso del modo perdido para dispositivos iOS supervisados

Puede activar y gestionar el modo perdido para dispositivos iOS supervisados. Si se pierde un dispositivo, la activación del modo perdido le permite:

- Bloquear el dispositivo y establecer el mensaje que desea mostrar (por ejemplo, puede mostrar la información de contacto para cuando alguien encuentre el dispositivo).
- Ver la ubicación actual del dispositivo sin necesidad de utilizar un perfil de servicio de ubicación.
- Controlar todos los dispositivos que se encuentren en el modo perdido desde la consola de gestión.

Activar modo perdido

El Modo perdido es compatible con los dispositivos iOS supervisados.

1. En la barra de menú, haga clic en **Usuarios > Dispositivos gestionados**.
2. Haga clic en el dispositivo para el desea activar el modo perdido.
3. En la pestaña 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**.

Localización de un dispositivo en modo perdido

Antes de empezar: Activar modo perdido

1. En la barra de menús, haga clic en **Usuarios > Dispositivos gestionados**.
2. Haga clic en un dispositivo que tiene el modo perdido activado.
3. En la pestaña Dispositivo, haga clic en **Obtener ubicación del dispositivo**.

Desactivar modo perdido

Antes de empezar: Activar modo perdido

1. En la barra de menús, haga clic en **Usuarios > Dispositivos gestionados**.
2. Haga clic en un dispositivo que tiene el modo perdido activado.
3. En la pestaña Dispositivo, haga clic en **Desactivar modo perdido**.

Bloqueo de activación en los dispositivos 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.

Para gestionar la función de bloqueo de activación en BlackBerry UEM:

- El dispositivo debe supervisarse.
- El dispositivo debe tener configurada una cuenta de iCloud.
- El dispositivo debe tener activada la opción Encontrar mi iPhone o Encontrar mi iPad.

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 forzar la activación utilizando la política de TI. Al activar el bloqueo de activación, BlackBerry 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.

Activar bloqueo de activación

Complete los siguientes pasos para activar el bloqueo de activación para cada dispositivo de forma individual. Si se aplica forzosamente el bloqueo de activación utilizando una regla de política de TI, ya estará activado.

Nota: Al activar la función Bloqueo de activación, puede tener lugar una breve demora entre BlackBerry UEM y Apple.

Antes de empezar:

- El dispositivo debe supervisarse.
- El dispositivo debe tener configurada una cuenta de iCloud.
- El dispositivo debe tener activada la opción Encontrar mi iPhone o Encontrar mi iPad.

1. En la barra de menús, haga clic en **Usuarios**.
2. Busque una cuenta de usuario.
3. En los resultados de la búsqueda, haga clic en el nombre de la cuenta de usuario.
4. Haga clic en la pestaña del dispositivo.
5. En la ventana **Administrar dispositivo** haga clic en **Activar bloqueo de activación**.

Después de terminar: Para ver la lista de códigos de desvío para dispositivos, consulte Visualice el código de desvío del bloqueo de activación

Desactivar bloqueo de activación

Complete los siguientes pasos para desactivar el bloqueo de activación para cada dispositivo de forma individual. Si se aplica forzosamente el bloqueo de activación utilizando una regla de política de TI, no podrá desactivarlo.

Nota: Al activar la función Bloqueo de activación, puede tener lugar una breve demora entre BlackBerry UEM y Apple.

1. En la barra de menú, haga clic en **Users**.
2. Busque una cuenta de usuario.

3. En los resultados de la búsqueda, haga clic en el nombre de la cuenta de usuario.
4. Haga clic en la pestaña del dispositivo.
5. En la ventana **Administrar dispositivo**, seleccione **Desactivar bloqueo de activación**.

Visualice el código de desvío del bloqueo de activación

Puede ver el código de desvío del bloqueo de activación y la fecha en la que se generó dicho código.

1. En la barra de menú, haga clic en **Usuarios > Bloqueo de activación de Apple**.
2. Busque un dispositivo.
3. En los resultados de búsqueda, haga clic en el dispositivo.
4. Si es necesario, desplácese a la derecha de la pantalla principal para ver el código de desvío.

Administración de las características de iOS mediante perfiles de carga personalizados

Se pueden utilizar perfiles de carga personalizados para controlar las funciones de dispositivos iOS que no están controladas por las políticas o perfiles de BlackBerry UEM.

Nota: Si una característica está controlada por una política o perfil de BlackBerry UEM, un perfil de carga personalizado puede que no funcione como se espera. Debería utilizar las políticas o perfiles actuales, siempre que sea posible.

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

- Controle una característica de iOS que no esté incluida en las políticas y los perfiles de BlackBerry UEM. Por ejemplo, con BES10, el asistente de CEO fue capaz de acceder tanto a su propia cuenta de correo como a la del CEO en un iPhone. En BlackBerry UEM, solo se puede asignar un perfil de correo a un dispositivo, de modo que el asistente solo puede tener acceso a su propia cuenta. Para resolver este problema, puede asignar un perfil de correo que permita al iPhone del asistente acceder a la cuenta de correo de este y a un perfil de carga personalizado que permita al iPhone de asistente acceder a la cuenta de correo del CEO.
- Controle una nueva característica de iOS que se lanzó después de la última versión de software de BlackBerry UEM. Por ejemplo, desea controlar una nueva característica que estará disponible para los dispositivos cuando actualicen a una versión reciente de iOS, pero BlackBerry UEM no tendrá un perfil para la nueva característica hasta la próxima versión de software de BlackBerry UEM. Para resolver este problema, puede crear un perfil de carga personalizado que controle esa función hasta la próxima versión de software de BlackBerry UEM.

Creación de un perfil de carga personalizado

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

1. En Apple Configurator, cree un perfil de configuración de Apple.
2. En la consola de administración de BlackBerry UEM, haga clic en **Políticas y perfiles**.
3. Haga clic en **Personalizada > Carga personalizada**.
4. Haga clic en +.
5. Escriba un nombre y una descripción para el perfil.
6. En Apple Configurator, copie el código XML para el 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>
```

7. En el campo **Carga personalizada**, pegue el código XML de Apple Configurator.
8. Haga clic en **Agregar**.

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

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 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 cuenta de Google para desbloquear un dispositivo que se ha restablecido a la configuración de fábrica. Se activa de forma predeterminada cuando un usuario agrega una cuenta 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.

Este perfil proporciona tres opciones:

- Puede desactivar la protección contra el restablecimiento de los datos de fábrica. Si desactiva la protección contra el restablecimiento de los datos de fábrica, cualquier particular podrá restablecer los ajustes 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 cuenta Google o si necesita restablecer un dispositivo propiedad de su empresa que se le ha devuelto.
- Los usuarios pueden utilizar credenciales de cuenta Google que ya están asociadas al dispositivo después de un restablecimiento 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 cuenta Google que ya están en el dispositivo. Esto evita que alguien con un dispositivo perdido o robado pueda restablecerlo y utilizarlo.
- Puede especificar las credenciales de cuenta 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. BlackBerry recomendamos que utilice esta opción únicamente si conoce a fondo la experiencia del usuario del dispositivo.

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

1. En la barra de menú, haga clic en **Políticas y perfiles > Dispositivos gestionados > Protección > Protección contra el restablecimiento de los datos de fábrica**.
2. Escriba un nombre y una descripción para el perfil.
3. Elija una **configuración de protección contra el restablecimiento de los datos de fábrica**. Seleccione 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 le pedirá a los usuarios que introduzcan un ID de usuario de Google cuando se restablezca la configuración de fábrica del dispositivo.
   - **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 predeterminada de fábrica del dispositivo mediante un método sin acreditación y una cuenta existente de Google en el dispositivo antes de que se produzca en restablecimiento, la cuenta deberá verificarse después del restablecimiento del dispositivo a la configuración de fábrica. Tenga en

cuenta que si su empresa utiliza una cuenta gestionada por una estructura de cuenta 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.

- **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, las credenciales de la cuenta de Google personal del usuario no se pueden utilizar después de un restablecimiento de fábrica.

4. 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 **+** > **Añadir utilizando la autenticación de Google** y, a continuación, inicie sesión en la cuenta de Google que desea utilizar para iniciar sesión en los dispositivos que se han restablecido.

   Puede añadir hasta 20 cuentas. También puede especificar la cuenta manualmente. Para obtener más información, consulte Obtención manual de un ID de usuario para una cuenta de Google.
5. 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 G Suite o Google Cloud, seleccione **Agregar una cuenta de Google creada por BlackBerry UEM** si desea incluir la cuenta de Google del trabajo del usuario en la lista de cuentas que pueden desbloquear el dispositivo después de un restablecimiento de fábrica.
6. Haga clic en **Guardar**.

Obtención manual de un ID de usuario para una cuenta de Google

Puede utilizar una cuenta de Google existente o crear una específicamente para usarla con protección contra el restablecimiento de los datos de fábrica. Si decide agregar una cuenta manualmente en lugar de utilizar la autenticación de Google, debe obtener el ID de usuario de la cuenta.

1. Diríjase al sitio de desarrolladores de Google People API (https://developers.google.com/people/api/rest/v1/people/get).
2. En el campo **resourceName**, escriba: people/me
3. En el campo **personalFields**, escriba: metadata
4. Haga clic en el botón de **ejecutar**.
5. En la pantalla para **elegir una cuenta**, seleccione la cantidad que desea utilizar para configurar el perfil de protección contra el restablecimiento de los datos de fábrica.
6. En la pantalla sobre que **el explorador de API de Google quiere acceder a su cuenta de Google**, haga clic en el botón de **permitir**.
7. En la parte derecha de la página de People ID, se mostrará el ID de usuario de 21 dígitos en el campo "id". Tenga en cuenta que el ID aparece debajo del encabezado verde con el número 200.

¿Cómo responde la protección contra el restablecimiento de los datos de fábrica ante los restablecimiento del dispositivo?

Existen varias formas en las que un dispositivo puede restablecer la configuración predeterminada de fábrica. En función del modo en que se restablezca el dispositivo, la protección contra el restablecimiento de los datos de fábrica responde de forma diferente. Para obtener más información acerca de restablecimientos seguros y poco seguros, visite support.blackberry.com/community y lea el artículo KB56972.

- La desactivación de BlackBerry UEM Client no se considera un restablecimiento seguro, ya que el usuario del dispositivo no se verifica antes de la desactivación. Por tanto, la protección contra el restablecimiento de los datos de fábrica se activa cuando el dispositivo se restablece y una vez completada la desactivación.
- Enviar el comando "Eliminar todos los datos del dispositivo" de la consola de administración puede ser un restablecimiento tanto seguro como poco seguro. Si selecciona la opción "Eliminar protección contra el restablecimiento de los datos de fábrica" cuando envíe el comando, la protección contra el restablecimiento de los datos de fábrica no se activará cuando se restablezca el dispositivo.
- Para restablecer el dispositivo desde la configuración de este, es necesario que el usuario se autentique antes del restablecimiento. Este se considera un restablecimiento seguro y la protección contra el restablecimiento de los datos de fábrica no se activa.
- Pueden utilizarse cargadores de arranque o herramientas de recuperación o depuración (ADB) para restablecer los valores predeterminados de fábrica del dispositivo y esto se considera poco seguro porque la identidad del usuario no se valida antes de que se realice el restablecimiento. Por lo tanto, la protección contra el restablecimiento de los datos de fábrica se activa cuando se restablece el dispositivo.

Consideraciones para el uso de una cuenta de Google Play gestionada específica cuando se configura un perfil de protección contra el restablecimiento de los datos de fábrica

Si su empresa utiliza una cuenta administrada de Google Play, puede que le interese considerar la posibilidad de utilizar la opción "Habilitar y especificar las credenciales de la cuenta de Google cuando se restablece el dispositivo a la configuración de fábrica" en el perfil de protección de restablecimiento de fábrica, ya que una cuenta de Google no está disponible en los dispositivos de su empresa que utiliza para restablecer la configuración de fábrica y, por tanto, la protección contra el restablecimiento de los datos de fábrica no está disponible en el dispositivo.

Si decide utilizar la opción "Habilitar y especificar las credenciales de la cuenta de Google cuando se restablece el dispositivo a la configuración de fábrica", existen varios factores que debe tener en cuenta:

- Asegúrese de que el ID de usuario de 21 dígitos que introduzca en el perfil sea el correcto. Si el número no coincide con la cuenta de Google de su empresa que desea utilizar, no existe forma de eliminar la protección contra el restablecimiento de los datos de fábrica del dispositivo una vez se haya activado. Para obtener más información, consulte Obtención manual de un ID de usuario para una cuenta de Google.
- En la política de TI de los usuarios de su empresa a quienes les asigne el perfil de protección contra el restablecimiento de los datos de fábrica, BlackBerry le recomienda que no seleccione la opción "Permitir restablecimiento de la configuración predeterminada de fábrica". Al desmarcar la opción, se desactiva la opción de restablecimiento de los datos de fábrica de la configuración del dispositivo y se desactiva el botón en BlackBerry UEM Client. Este botón garantiza que los usuarios no utilicen la opción de desactivación sin acreditación en UEM Client, que siempre da lugar a la protección contra el restablecimiento de los datos de fábrica del dispositivo. Si esta opción está activada, los usuarios deben ponerse en contacto con el administrador de BlackBerry UEM de su empresa para restablecer sus dispositivos.
- Proporcione información a los usuarios de su empresa sobre la protección contra el restablecimiento de los datos de fábrica del dispositivo y el procedimiento que se utilizará para desactivar la protección contra el restablecimiento de los datos de fábrica cuando esté activada en el dispositivo. Para obtener más información, consulte la sección Eliminación de la protección contra el restablecimiento de los datos de fábrica de un dispositivo. El administrador de BlackBerry UEM debe elegir si desea proporcionar la información de la cuenta a los usuarios para eliminar el la protección contra el restablecimiento de los datos de fábrica o si los usuarios tendrán que solicitar soporte al personal local para desbloquear el dispositivo.

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

Cuando se habilita la protección contra el restablecimiento de los datos de fábrica en el dispositivo, la activación de la empresa en BlackBerry UEM dejará de funcionar. Primero, debe eliminarla protección contra el restablecimiento de los datos de fábrica utilizando la configuración inicial de Android

1. Si está utilizando cualquier forma de sistema de activación automatizada (como el aprovisionamiento automático o Samsung Knox Mobile Enrollment), debe desactivar dicha forma 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 le 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 y la contraseña de la cuenta de Google, se le preguntará si desea añadir este 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 'afw#blackberry' o los datos de la cuenta de Google de la empresa para instalar BlackBerry UEM Client y volver a activar el dispositivo frente a BlackBerry 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 volver a activarse con la empresa.
   - Dispositivos con aprovisionamiento automático o Samsung Knox Mobile Enrollment: si está utilizando cualquier forma de sistema de activación automática (como el aprovisionamiento automático o Samsung Knox Mobile Enrollment), puede volver a activar esta forma 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 Windows Information Protection para dispositivos con Windows 10

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

- Separar los datos personales y del trabajo en los dispositivos y poder borrar solo los datos de trabajo
- 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 memoria USB
- Auditar el comportamiento de los usuarios y realizar las acciones correspondientes para evitar pérdidas de datos

Al configurar WIP para los dispositivos, puede especificar las aplicaciones que desea proteger con WIP. 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. Para obtener más información sobre WIP, visite https://docs.microsoft.com/es-es/windows/security/information-protection/windows-information-protection/protect-enterprise-data-using-wip.

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 del trabajo. Para obtener más información sobre las aplicaciones habilitadas e inhabilitadas, visite https://docs.microsoft.com/es-es/windows/security/information-protection/windows-information-protection/enlightened-microsoft-apps-and-wip.

Creación de un perfil de Windows Information Protection

1. En la barra de menú, haga clic en **Políticas y perfiles**.
2. Haga clic en **Protección > Windows Information Protection**.
3. Haga clic en +.
4. Escriba un nombre y una descripción para el perfil.
5. Configure los valores adecuados para la configuración de cada perfil. Para obtener más información acerca de la configuración de cada perfil, consulte Windows 10: configuración de perfil de Windows Information Protection.
6. Haga clic en **Agregar**.

Windows 10: configuración de perfil de Windows Information Protection

Windows 10: configuración de perfil de Windows Information Protection	Descripción
Configuración de Windows Information Protection	Esta configuración especifica si se ha activado Windows Information Protection y el nivel de aplicación. Cuando esta configuración está definida en "Desactivado", no se cifran los datos y se desactiva el registro de auditoría. Cuando esta configuración se establece en "Silencio", los datos se cifran y se registra cualquier intento de compartir datos protegidos. Cuando esta configuración se establece en "Anulación", los datos se cifran, se avisa al usuario cuando intenta compartir datos protegidos y se registra cualquier intento de compartir datos protegidos. Cuando esta configuración se establece en "Bloqueo", los datos se cifran, los usuarios no pueden compartir datos protegidos y se registra cualquier intento de compartir datos protegidos. Valores posibles: • Desactivado • Silencio • Anulación • Bloqueo El valor predeterminado es "Desactivado".
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. Puede separar varios dominios con canalizaciones con barras verticales (|). El primer dominio se utiliza como una cadena para etiquetar los archivos que están protegidos por las aplicaciones que utilizan WIP. Por ejemplo, `example.com|example.net`.
Archivo de certificado de recuperación de datos (.der, .cer)	Esta configuración especifica el archivo de certificado de recuperación de datos. El archivo que especifique debe contar con un certificado codificado mediante PEM o DER con una extensión de archivo .der o .cer. Utilice el archivo de certificado de recuperación de datos para recuperar archivos que estaban protegidos localmente en un dispositivo. Por ejemplo, si su empresa desea recuperar datos protegidos por WIP de un dispositivo. Para obtener información sobre un certificado de recuperación de datos, consulte la documentación de Microsoft Windows Information Protection.
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.

Windows 10: configuración de perfil de Windows Information Protection	Descripción
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. De manera predeterminada, la opción no está seleccionada.
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 cuando se conecta al dominio enumerado 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.
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.

Windows 10: configuración de perfil de Windows Information Protection	Descripción
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. Por ejemplo, `example.com,example.net`.

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 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>`
	
	Para obtener más información sobre el uso de AppLocker, consulte la documentación de Microsoft AppLocker.

Windows 10: configuración de perfil de Windows Information Protection	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 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>`
	
	Para obtener más información sobre el uso de AppLocker, consulte la documentación de Microsoft AppLocker.

Windows 10: configuración de perfil de Windows Information Protection	Descripción
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".
Recopilar registros de auditoría del dispositivo	En la configuración se especifica si desea recopilar registros de auditoría del dispositivo.

Activación del cifrado BitLocker en dispositivos con Windows 10

El cifrado de unidad BitLocker es una función de protección de datos del sistema operativo que ayuda a mitigar el acceso no autorizado a datos cuando un dispositivo se pierde o es robado. Puede activar el cifrado BitLocker en dispositivos con Windows 10 y la protección se refuerza si el dispositivo también cuenta con un módulo de plataforma segura (TPM), lo que le proporciona la opción de solicitar una autenticación adicional en el inicio (por ejemplo, una clave de inicio, un PIN o una unidad USB extraíble). En BlackBerry UEM también puede crear un perfil de conformidad para evitar que los usuarios desactiven BitLocker y así imponer su uso en aquellos dispositivos que requieran el cifrado.

Puede configurar las opciones de recuperación para acceder al sistema operativo o a las unidades de datos protegidos por BitLocker. Los usuarios pueden acceder a claves de recuperación desde la consola de Active Directory y, si está habilitado, se pueden hacer copias de seguridad de las contraseñas de recuperación en los Active Directory Domain Services para que el administrador pueda recuperarlas utilizando la herramienta Visor de contraseñas de recuperación de BitLocker.

Configure las siguientes reglas de políticas de TI de UEM para permitir la compatibilidad con el cifrado de BitLocker en los dispositivos con Windows 10:

- Método de cifrado BitLocker para escritorio
- Permitir que el cifrado de la tarjeta de memoria pregunte al dispositivo
- Permitir que el cifrado de unidad BitLocker active la codificación en el dispositivo
- Establecer métodos de cifrado predeterminados para cada tipo de unidad
- Requerir autenticación adicional al iniciar
- Requerir longitud mínima del PIN para el inicio
- URL y mensaje de recuperación previos al arranque
- Opciones de recuperación para la unidad del sistema operativo de BitLocker
- Opciones de recuperación de BitLocker para unidades de disco fijas
- Requerir la protección de BitLocker para las unidades de datos fijas
- Requerir la protección de BitLocker para las unidades de datos extraíbles
- Permitir pregunta de ubicación de la clave de recuperación
- Activar el cifrado para los usuarios estándar

Para obtener más información acerca de las reglas de políticas de TI de BitLocker, consulte la hoja de cálculo de referencia de políticas.

Administración de atestación para 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 siguientes dispositivos:

- Dispositivos con Samsung Knox
- Dispositivos con Android
- Dispositivos con Windows 10

Administración de los dispositivos con Samsung Knox

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

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

1. En la barra de menú, haga clic en **Configuración > Configuración general > Atestación**.
2. Para activar la atestación en los dispositivos con Samsung Knox, seleccione **Activar las comprobaciones de atestación periódicas para los dispositivos con KNOX Workspace**.
3. En la sección **Frecuencia de la comprobación**, especifique, en días o en horas, la frecuencia con la que el dispositivo debe devolver una respuesta de atestación a BlackBerry UEM.
4. En la sección **Periodo de gracia**, especifique un periodo de gracia. Después de que caduque el periodo de gracia sin respuesta de atestación, se considera que el dispositivo no cumple los requisitos y está sujeto a las condiciones especificadas en el perfil de cumplimiento que se asigna al usuario. Tenga en cuenta que si un dispositivo de un usuario está fuera de cobertura, apagado o sin batería, no puede responder a las comprobaciones de atestación que envía BlackBerry UEM y, por tanto, BlackBerry UEM considerará que el dispositivo no cumple con los requisitos. Si ha configurado la política de cumplimiento de su empresa para que borre el dispositivo cuando no cumpla los requisitos, en caso de que el dispositivo no responda antes de que caduque el periodo de gracia, se eliminarán los datos del dispositivo.
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

Gestión de atestaciones de dispositivos Android y aplicaciones de BlackBerry Dynamics mediante SafetyNet

Al utilizar la atestación de SafetyNet de Android, BlackBerry UEM realiza comprobaciones para probar la autenticidad y la integridad de los dispositivos y las aplicaciones de BlackBerry Dynamics Android de su entorno empresarial. SafetyNet 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, además de la detección de utilización y origen existente de BlackBerry. Para obtener más información sobre SafetyNet, consulte la información de Google.

BlackBerry UEM realiza la atestación de SafetyNet en las siguientes circunstancias:

- Tras la activación del dispositivo cuando BlackBerry UEM Client está instalado

- Durante la activación del dispositivo cuando BlackBerry UEM Client está instalado
- Durante la activación de las aplicaciones de BlackBerry Dynamics
- Tras la activación de aplicaciones de BlackBerry Dynamics
- A petición mediante API de REST
- En el reinicio del dispositivo si BlackBerry UEM Client está activado

Consideraciones para configurar la atestación de SafetyNet

- La opción de error de atestación de Google SafetyNet es una configuración del perfil de conformidad de los dispositivos Android y las aplicaciones de BlackBerry Dynamics que le permite especificar las acciones que se llevarán a cabo si los dispositivos o las aplicaciones no superan la atestación de SafetyNet. Para configurar esta opción, acceda a la pestaña **Políticas y perfiles > Conformidad > Android**.
- Si no habilita la regla de conformidad de "Error de atestación de Google SafetyNet", no se aplicarán las acciones de conformidad a las aplicaciones que ya estén activadas.
- Cuando habilita SafetyNet, se lleva a cabo la atestación durante la activación; no puede utilizar una política para aplicar la atestación durante la activación.
- No es necesario BlackBerry UEM Client para habilitar la atestación de SafetyNet.
- BlackBerry UEM Client no aparece en la lista de aplicaciones de BlackBerry Dynamics que puede configurar para la atestación de SafetyNet. BlackBerry UEM envía comprobaciones de atestación a BlackBerry UEM Client y recibe respuestas.
- BlackBerry UEM realiza comprobaciones de atestación a cada aplicación de BlackBerry Dynamics que configure.
- BlackBerry UEM no confía en versiones anteriores de las aplicaciones. Por ejemplo, si quiere habilitar las comprobaciones de atestación para BlackBerry Work, debe asegurarse de que la versión de BlackBerry Work de los dispositivos de su empresa sea la más reciente. De lo contrario, se producirá un error en las nuevas activaciones. Tenga en cuenta que, hasta que no habilite la opción "Error de atestación de Google SafetyNet" en el perfil de conformidad de su empresa, aunque sus usuarios activados existentes utilicen versiones anteriores de aplicaciones, no se llevarán a cabo acciones adversas en aplicaciones ni dispositivos.
- Además de la activación y la atestación periódica, BlackBerry UEM utiliza nuevas API de REST que le permiten crear flujos de trabajo de servidor personalizados. Por ejemplo, si una aplicación necesita acceder a un determinado elemento seguro y remoto, antes de conceder el acceso, el servidor de aplicaciones se comunica con BlackBerry UEM para aplicar la atestación de SafetyNet en la aplicación o el dispositivo.
- Si el dispositivo de un usuario está fuera de cobertura, apagado o sin batería, no puede responder a las comprobaciones de atestación que envía BlackBerry UEM y, por tanto, BlackBerry UEM considerará que el dispositivo no cumple con los requisitos. Si ha configurado la política de cumplimiento de su empresa para que borre el dispositivo cuando no cumpla los requisitos, en caso de que el dispositivo no responda antes de que caduque el periodo de gracia, se eliminarán los datos del dispositivo cuando este se conecte a una red inalámbrica.
- Si configura un plazo en el campo de periodo de gracia de la aplicación, solo se realizarán cambios en las aplicaciones que no respondan en el plazo que establezca. Por ejemplo, si establece el valor del periodo de gracia de la aplicación en 7 días, y sus usuarios utilizan BlackBerry Work a diario, pero no utilizan BlackBerry Tasks en los 7 días, solo se realizarán cambios en BlackBerry Tasks.
- Si añade una nueva aplicación a BlackBerry UEM y se produce un error en la atestación durante la activación, la aplicación no se activará, independientemente de la opción que haya configurado en la sección "Error de atestación de Google SafetyNet" del perfil de conformidad de su empresa. Si una aplicación ya se ha activado, está sujeta a las reglas que haya especificado en el perfil de conformidad.
- Los usuarios de su empresa deben tener instalada la versión más reciente de los servicios de Google Play.
- Si se produce un error en la atestación de un dispositivo, no se muestra ninguna indicación del error en la columna de OS en peligro de la página de dispositivos gestionados.
- Para obtener más información sobre el desarrollo de aplicaciones de BlackBerry Dynamics para dispositivos Android, consulte el contenido de Desarrollador.

Configuración de atestaciones de dispositivos Android y aplicaciones de BlackBerry Dynamics mediante SafetyNet

1. En la barra de menú, haga clic en **Configuración > Configuración general > Atestación**.
2. Para activar la atestación en los dispositivos Android, seleccione **Activar las comprobaciones de atestación periódicas con SafetyNet**.
3. Seleccione **Activar coincidencia de perfil CTS** si desea activar el conjunto de pruebas de compatibilidad de Google. Para obtener más información sobre CTS, consulte la información de Google.
4. En la sección **Frecuencia de la comprobación**, especifique, en días o en horas, la frecuencia con la que el dispositivo debe devolver una respuesta de atestación a BlackBerry UEM. Consideraciones para la configuración de la frecuencia de la comprobación:
   - Aunque puede configurar la frecuencia con la que BlackBerry UEM comprueba la autenticidad e integridad del dispositivo, es obligatorio realizar una atestación durante la activación de la aplicación.
   - Si ha implementado BlackBerry UEM Client, se añadirá como una de las aplicaciones que BlackBerry UEM comprueba para la atestación de SafetyNet automáticamente.
   - El dispositivo BlackBerry UEM Client utiliza un canal de comunicación diferente para BlackBerry UEM que otras aplicaciones BlackBerry Dynamics, que deberá ejecutarse y autorizarse para poder conectarse a BlackBerry UEM y recibir actualizaciones de políticas. BlackBerry UEM puede comunicarse de forma proactiva con BlackBerry UEM Client e iniciar la aplicación si no se está ejecutando. SI configura una frecuencia de la comprobación de tres horas, BlackBerry UEM se comunicará con BlackBerry UEM Client cada tres horas y se realizará la comprobación de atestación. Sin embargo, los comandos de la aplicación BlackBerry Dynamics se almacenarán hasta que la aplicación se conecte a BlackBerry UEM y solo se almacenará el último comando de atestación. Si la aplicación no se usa durante 24 horas, cuando el usuario la inicie, solo se realizará una comprobación de atestación.
5. En la sección **Periodo de gracia**, especifique un periodo de gracia. Después de que caduque el periodo de gracia sin respuesta de atestación, se considera que el dispositivo no cumple los requisitos y está sujeto a las condiciones especificadas en el perfil de cumplimiento que se asigna al usuario. Así, si el dispositivo de un usuario está fuera de cobertura, apagado o sin batería, no puede responder a las comprobaciones de atestación que envía BlackBerry UEM y, por tanto, BlackBerry UEM considerará que el dispositivo no cumple con los requisitos. Si ha configurado la política de cumplimiento de su empresa para que borre el dispositivo cuando no cumpla los requisitos, en caso de que el dispositivo no responda antes de que caduque el periodo de gracia, se eliminarán los datos del dispositivo cuando este se conecte a una red inalámbrica.
6. En la sección **Periodo de gracia de gracia de aplicación**, especifique un periodo de gracia. Cuando caduque el periodo de gracia, las aplicaciones de BlackBerry Dynamics estarán sujetas a las condiciones especificadas en el perfil de cumplimiento asignado al usuario. El periodo de gracia se aplica según la aplicación. Tenga en cuenta que si solo ha asignado el BlackBerry UEM Client al dispositivo, se ignorará el periodo de gracia. Asimismo, BlackBerry UEM Client no aparece en la lista de aplicaciones de BlackBerry Dynamics Cuando agrega aplicaciones de BlackBerry Dynamics a la lista de aplicaciones que estarán sujetas a las comprobaciones de atestación, se aplican las siguientes reglas:
   - Solo las aplicaciones de esta lista se envían a las comprobaciones de atestación.
   - Solo las aplicaciones de esta lista se evalúan para la comprobación del periodo de gracia de la aplicación.
   - Solo las aplicaciones de esta lista están sujetas a una atestación durante la activación de la aplicación.

     Nota: Solo las aplicaciones de BlackBerry Dynamics que se han desarrollado específicamente para SafetyNet aparecerán en la lista. Para obtener más información, consulte el contenido de Desarrolladores.
7. Para agregar una aplicación que estará sujeta a las comprobaciones de atestación, haga clic en **+**.
8. Lleve a cabo una de estas acciones:
   - Haga clic en el nombre de una aplicación que ya figure en la lista.
   - Busque y seleccione el nombre de la aplicación.
9. Haga clic en **Seleccionar**.

10. Haga clic en **Guardar**.

Administración de los dispositivos con Windows 10

Al activar la atestación, BlackBerry UEM envía comprobaciones para probar la autenticidad y la integridad de los dispositivos Windows 10. El dispositivo se comunica con el Servicio de atestación de mantenimiento de Microsoft para comprobar la conformidad en función de la configuración que haya establecido en el perfil de conformidad de su empresa.

Nota: La configuración de atestación de Windows 10 no se aplica a BlackBerry Desktop (BlackBerry Access + BlackBerry Work).

1. En la barra de menú, haga clic en **Configuración > Configuración general > Atestación**.
2. Para activar la atestación en los dispositivos con Windows 10, seleccione **Activar las comprobaciones de atestación periódicas para los dispositivos Windows 10**.
3. En la sección **Frecuencia de la comprobación**, especifique, en días o en horas, la frecuencia con la que el dispositivo debe devolver una respuesta de atestación a BlackBerry UEM.
4. En la sección **Periodo de gracia**, especifique un periodo de gracia. Después de que caduque el periodo de gracia sin respuesta de atestación, se considera que el dispositivo no cumple los requisitos y está sujeto a las condiciones especificadas en el perfil de cumplimiento que se asigna al usuario. También se debe tener en cuenta que si el dispositivo de un usuario está fuera de cobertura, apagado o sin batería, no puede responder a las comprobaciones de atestación que envía BlackBerry UEM y, por tanto, BlackBerry UEM considerará que el dispositivo no cumple con los requisitos. Si ha configurado la política de cumplimiento de su empresa para que borre el dispositivo cuando no cumpla los requisitos, en caso de que el dispositivo no responda antes de que caduque el periodo de gracia, se eliminarán los datos del dispositivo.
5. Haga clic en **Guardar**.

Puede ver cualquier infracción de conformidad en la página de detalles del dispositivo.

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

Migre dispositivos iOS para utilizar un canal protegido

Realice estos pasos para exportar una lista de dispositivos que aún no están utilizando un canal protegido. Durante la migración, los dispositivos se reactivarán y los usuarios pueden verse afectados, por ejemplo, con la reinstalación de aplicaciones y perfiles de trabajo. Para obtener más información, visite support.blackberry.com/kb y lea el artículo KB99869.

Nota: En dispositivos inscritos con DEP, la configuración de inscripción de DEP no se migra y los dispositivos perderán la configuración de inscripción en el entorno de destino. Los usuarios deben restablecer los dispositivos a los valores de fábrica y, a continuación, reactivar BlackBerry UEM Client después de la migración. Para obtener más información, visite support.blackberry.com y lea el artículo KB 100525.

1. En la barra de menú de la consola de gestión, haga clic en **Configuración > Migración > Canal protegido de iOS**.
2. Haga clic en **Exportar**. Se descarga una lista de dispositivos que no están utilizando aún un canal protegido. Tenga en cuenta que los dispositivos que se encuentran en grupos de dispositivos compartidos se incluyen en la exportación solo con fines informativos. Estos dispositivos se omitirán durante la importación y los usuarios deberán restablecer los valores de fábrica del dispositivo y, a continuación, reactivar BlackBerry UEM Client.
3. Haga clic en **Examinar** y desplácese hasta el archivo que contiene las cuentas de usuario que desea migrar. Tenga en cuenta que si la lista que descargó en el paso 2 contiene más de 1000 entradas, debe dividir las entradas entre los archivos que cargue para que contengan 1000 entradas como máximo y cargar varios archivos.

Migrar un dispositivo iOS para utilizar un canal protegido

Puede migrar dispositivos individuales para utilizar un canal protegido.

1. Busque el dispositivo que desea migrar.
2. En la sección Administrar dispositivo, haga clic en **Migrar a canal protegido de iOS**.
3. Haga clic en **Submit**.

Exportar una lista de dispositivos macOS que requieran reactivación para utilizar un canal protegido

Lleve a cabo estos pasos para exportar una lista de los dispositivos afectados por el problema de seguridad comunicado en el artículo KB99869. Cada usuario que tenga un dispositivo que aparezca en el archivo que exporte debe reactivar su dispositivo en el portal de autoservicio.

1. Vaya a **Ajustes > Migración > Canal protegido de macOS**.
2. Haga clic en **Exportar**. Se descargará una lista de dispositivos que deben reactivarse.
3. Póngase en contacto con los usuarios que tienen dispositivos en la lista y pídales que reactiven sus dispositivos en el portal de autoservicio. Para obtener información sobre la reactivación en el portal de autoservicio, consulte la Guía del usuario.

Aviso legal

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

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

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

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

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

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

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

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

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

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

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

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

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

Publicado en Canadá