IBM MaaS360 Mobile Device Management para iOS

Aprovisione, gestione y proteja los dispositivos, las apps y los contenidos iOS más recientes

Principales ventajas

- Aprovisione, proteja y gestione sus dispositivos, apps y contenidos desde una consola única
- Configure el correo electrónico, el calendario, los contactos, la Wi-Fi y los perfiles VPN mediante el protocolo OTA para incorporar usuarios rápidamente
- Disfrute de soporte técnico desde el día de lanzamiento para las últimas versiones de los sistemas operativos móviles de los dispositivos iOS
- Defina políticas de seguridad y aplíquelas con acciones de cumplimiento automáticas, por ejemplo, solicitando un código de acceso al dispositivo o bloqueando los dispositivos vulnerables
- Utilice paneles de control robustos e informes para gestionar dispositivos corporativos y personales

Apple + IBM® MaaS360® = mejor juntos

Apple sigue innovando en tecnologías para empresas para que iOS 9 se convierta en una plataforma de productividad más potente. Y MaaS360 ofrece un soporte rápido y robusto para iOS 9 y las versiones anteriores. Trabajando de forma conjunta, IBM y Apple están ayudando a que las organizaciones se den cuenta del potencial sin explorar de la movilidad con sus empleados, clientes y socios.

Inscriba y actualice dispositivos a la última versión de iOS instantáneamente y sin problemas el día de lanzamiento de Apple sin interrupciones de usuario ni problemas de TI. No se quede atrás con otros proveedores de gestión de dispositivos móviles (MDM); ¡disfrute hoy mismo de muchas de las nuevas funciones de iOS 9 con MaaS360!

Gestión Apple iOS instantánea

IBM MaaS360 para iOS ofrece mayor visibilidad y control para facilitar la compatibilidad con iPhones y iPads en la empresa, y que sean compatibles con versiones iOS 4.3 y superiores. Actualmente, es compatible con iOS 9 y ofrece herramientas que puede usar para obtener información, realizar acciones, establecer y distribuir políticas, gestionar apps y documentos y mucho más.

La solución ofrece una manera rápida y sencilla para proteger estos dispositivos y los datos corporativos que contienen. Puede inscribirlos mediante el protocolo OTA y usar políticas de seguridad y reglas de cumplimiento para imponer códigos de acceso y cifrado, detectar y restringir los dispositivos liberados, apps de listas blancas o listas negras, controlar las copias de seguridad de archivos y mucho más.

Figura 1: Simplemente, implante apps y contenidos en los dispositivos iOS de su organización

Obtener información

- Modelo, número de serie, sistema operativo
- Red doméstica/red actual
  - Estado del roaming, dirección MAC
- Cantidad de almacenamiento libre
- Apps, versiones y tamaño
- ID del dispositivo (número de teléfono, IMEI, dirección de correo electrónico)
  - Nivel de cifrado, detección de dispositivos liberados, estado del código de acceso, restricciones de dispositivos, perfiles instalados, políticas de seguridad y mucho más
- Use DEP para inscribir automáticamente dispositivos de la empresa durante la activación con sus configuraciones y políticas
- El Bloqueo de Activación de Buscar mi iPhone está activado, por lo que hará falta la ID de Apple del usuario para desbloquear el dispositivo
- Informe si existe una cuenta de iTunes en un dispositivo
- Vea informes exhaustivos sobre documentos, usuarios, dispositivos y apps, entre otros

Realizar acciones

- Configure los ajustes y perfiles de la Wi-Fi, la VPN y el correo electrónico
- Localice, llame, bloquee un dispositivo o restablezca contraseñas olvidadas
- Limpie de forma selectiva datos corporativos a la vez que mantiene los datos personales de un dispositivo de un empleado
- Realice un borrado completo de un dispositivo perdido o robado
- Cambie la política de iOS
- Active o desactive los controles de roaming de datos y voz

Catálogo de aplicaciones empresariales

- Facilidad de gestión de apps de empresa: Las apps móviles distribuidas por MaaS360 para dispositivos iOS se pueden gestionar totalmente, lo que le permite simplificar las implementaciones de apps al mismo tiempo que aumenta la seguridad
  - Recomiende apps de iTunes para empleados
  - Distribuya apps “caseras” y publique actualizaciones
  - Envíe una notificación push de una app a un dispositivo de forma remota; instale en modalidad silenciosa en caso de que el dispositivo esté supervisado
  - Gestione los controles Open In para restringir la apertura de archivos desde las apps corporativas a las apps personales y viceversa
  - Conecte apps gestionadas a la VPN para un acceso a la red protegido
  - Permita un inicio de sesión único entre apps para autenticación
  - Aplique un cifrado de datos de apps de terceros automáticamente
- Soporte del Programa de Compras por Volumen (VPP) de Apple
  - Distribuya e instale apps de prepago sin visitar la Apple App Store
  - Ahorre dinero al conservar la propiedad y el control total de las licencias VPP de apps y libros cuando los usuarios no los necesiten más

Establecer y distribuir políticas

- Aplique requerimientos de códigos de acceso
- Configure restricciones de dispositivos
  - Aplique copias de seguridad cifradas
  - Restrinja el uso de cámaras, FaceTime, Touch ID y otras aplicaciones
  - Restrinja la instalación de apps, Photo Stream compartido y otras aplicaciones
  - Obligue al tráfico de internet a pasar a través de un servidor proxy HTTP global
  - Distribuya perfiles Wi-Fi, VPN y de correo electrónico, como los ajustes de Exchange ActiveSync
- Gestione los controles de iCloud
  - Gestione documentos, datos de apps, copias de seguridad y sincronización de fotos del dispositivo con iCloud para usuarios, grupos o todos los dispositivos
- Aumente la seguridad del correo electrónico
  - Restrinja el movimiento de correos electrónicos de los usuarios entre cuentas y protéjase contra la filtración de datos corporativos
  - Evite que apps de terceros envíen correos electrónicos
- Configuración Wi-Fi avanzada
  - Gestione y envíe notificaciones push de la configuración proxy y autoconexión de SSID
- Aplicación de contraseña en iTunes
  - Solicite a los usuarios que introduzcan su contraseña de iTunes para acceder al contenido, las apps y los datos almacenados en iTunes
- Envíe un mensaje y un número en la pantalla de bloqueo si pierde el dispositivo
- Permita la función Transferencia, que permite continuidad, resultados web en sincronización con Spothlight y iCloud para las apps gestionadas

Soporte técnico desde el día de lanzamiento

Juntos, iOS 9 y MaaS360, están listos para ofrecer un nivel completamente nuevo de seguridad, productividad y funciones de gestión de datos y dispositivos para ayudar a su organización a dar el siguiente paso en su viaje hacia la movilidad.

Nuevas funciones de seguridad empresarial de iOS 9

- Restrinja AirDrop para las apps gestionadas y la biblioteca de fotografías de iCloud
- Establezca nuevas restricciones supervisadas para el uso de la App Store, atajos de teclado, Apple Watch, modificación de contraseñas, descargas automáticas de apps y mucho más
- Desactivar la notificación de fiabilidad de apps de empresa en dispositivos supervisados

Nuevas funciones de distribución de apps de iOS 9

- La distribución de apps basada en dispositivos implanta las apps directamente en los dispositivos que utilizan el Programa de Compras por Volumen (VPP) y MaaS360 para asignar apps directamente a un dispositivo con el número de serie, sin la necesidad de un ID de Apple
- Envíe notificaciones push o extraiga apps públicas sin la necesidad de que el usuario acceda a la App Store
- Las apps de empresa instaladas con MaaS360 son explícitamente de confianza; ya no necesita la confirmación de confianza del usuario
- Si un dispositivo tiene una app antes de su supervisión, esta se gestionarán en modalidad silenciosa cuando se supervise el dispositivo
- Las apps compradas y distribuidas a través de VPP se pueden asignar a dispositivos o usuarios en cualquier país en el que estén disponibles

Nueva gestión de datos y dispositivos de iOS 9

- MaaS360 puede activar actualizaciones del dispositivo a las nuevas versiones iOS para cualquier dispositivo del Programa de inscripción de dispositivos (DEP)
- Apple Configurator le permite preimplantar apps y transmitir la inscripción de dispositivos con MaaS360 a través de DEP
- VPN Per App es compatible con UDP y TCP para la transmisión de audio o vídeo

Para obtener más información acerca de IBM MaaS360 y descargar una versión de prueba de 30 días sin coste alguno, visite www.ibm.com/maas360

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Creado en los Estados Unidos de América
Abril de 2016

Este documento está actualizado en la fecha de publicación original y puede ser modificado por IBM en cualquier momento. No todas las ofertas están disponibles en todos los países en los que opera IBM.

Los datos de rendimiento y ejemplos de clientes que se citan se presentan solo a título ilustrativo. Los resultados de rendimiento reales pueden variar en función de las configuraciones y condiciones operativas específicas. Es responsabilidad del usuario evaluar y verificar la operación de cualquier otro producto o programa con los productos y programas IBM.

LA INFORMACIÓN CONTENIDA EN ESTE DOCUMENTO SE PROPORCIONA “TAL CUAL”, SIN GARANTÍA ALGUNA, EXPRESA NI IMPLÍCITA, INCLUIDAS LAS GARANTÍAS DE COMERCIABILIDAD E IDONEIDAD PARA UN FIN DETERMINADO, NI NINGUNA GARANTÍA O CONDICIÓN DE NO CONTRAVENCIÓN. Los productos IBM están garantizados de acuerdo con los términos y condiciones de los acuerdos en virtud de los cuales se proporcionen.

El cliente es responsable de asegurarse del cumplimiento de las leyes y normas que sean de aplicación. IBM no proporciona asesoramiento legal ni declara o garantiza que sus productos o servicios asegurarán que el cliente cumpla alguna ley o norma determinada.

Las declaraciones en cuanto a futuras direcciones y propósitos de IBM están sujetas a cambios o cancelaciones sin previo aviso y solo representan metas y objetivos.

Declaración de buenas prácticas de seguridad: La seguridad de un sistema de TI implica proteger los sistemas y la información mediante prevención, detección y respuesta ante accesos indebidos desde el interior y el exterior de su empresa. Un acceso indebido puede dar como resultado la alteración, destrucción o apropiación indebida de la información o puede originar daños o el uso indebido de sus sistemas, incluido el ataque a otros. No existe ningún sistema o producto de TI que se pueda considerar totalmente seguro, ni existe ningún producto o medida de seguridad que sea completamente eficaz en la prevención de accesos indebidos. Los sistemas y productos IBM están diseñados para formar parte de un enfoque de seguridad global, lo que necesariamente implica procedimientos operativos adicionales, y pueden necesitar otros sistemas, productos o servicios para ser más eficaces. IBM no garantiza que los sistemas y productos sean inmunes a usos malintencionados o ilícitos de alguna parte.

Por favor, recicle

WGD03066-ESES-00