IBM MaaS360 Mobile Device Management for iOS

Prepare, proteja y gestione los dispositivos más actuales, las aplicaciones y el contenido en iOS

Principales ventajas

- Prepare, proteja y gestione sus dispositivos, aplicaciones y contenidos desde una única consola
- Configure el correo electrónico, calendario, contactos, Wi-Fi y perfiles de VPN por aire para incorporar rápidamente a los usuarios
- Experimente soporte de día de lanzamiento para las últimas versiones del sistema operativo para dispositivos iOS
- Establezca políticas de seguridad y aplíquelas con acciones de cumplimiento automatizadas, como exigir una clave de acceso para un dispositivo y bloquear un dispositivo comprometido
- Use tableros robustos e informes para administrar los dispositivos corporativos y los personales

Apple + IBM® MaaS360® = mejor juntas

Apple continúa innovando en tecnologías de nivel empresario para hacer de iOS 9 una plataforma de productividad más poderosa. Y MaaS360 brinda soporte rápido y robusto para iOS 9 y versiones anteriores. Al trabajar juntas, Apple + IBM están ayudando a las organizaciones a comprobar el potencial de movilidad sin explotar con sus empleados, clientes y asociados.

Inscriba y actualice dispositivos con la última versión de iOS de manera instantánea y perfecta el día de lanzamiento por Apple sin trastornos con los usuarios o problemas en TI. No quede rezagado con otros proveedores de gestión de dispositivos móviles (MDM); ¡experimente muchas de las nuevas características de iOS9 hoy mismo con MaaS360!

Gestión al instante de Apple iOS

IBM MaaS360 for iOS provee extensa visibilidad y control para soportar iPhones y iPads en la empresa, con compatibilidad para versiones de iOS 4.3 y superiores. Actualmente es compatible con iOS 9, y proporciona herramientas que usted puede usar para obtener detalles, llevar a cabo acciones, establecer y distribuir políticas, gestionar aplicaciones y documentos y mucho más.

La solución brinda una manera rápida y fácil de proteger estos dispositivos y los datos corporativos que contienen. Puede inscribirlos por aire (OTA) y usar políticas de seguridad y reglas de cumplimiento para imponer contraseñas y cifrado, detectar y restringir dispositivos liberados (jailbroken), incluir aplicaciones en listas blancas o listas negras, controlar copias de respaldo de archivos y mucho más.

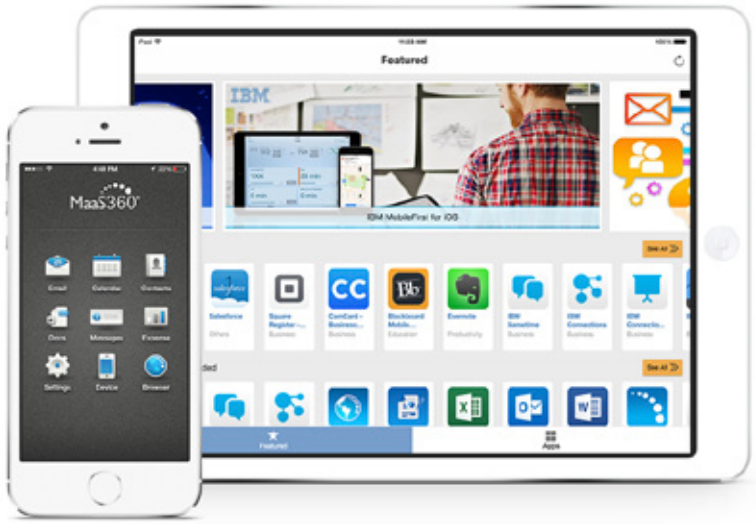

Figura 1: Implemente simplemente aplicaciones y contenido en los dispositivos iOS de su organización

Obtener detalles

- Modelo, número de serie, sistema operativo
- Red hogareña/red actual
  - Estado de "roaming", dirección MAC
- Cantidad de almacenamiento libre
- Aplicaciones, versiones y tamaño
- ID de dispositivo (número de teléfono, IMEI, dirección de correo electrónico)
  - Nivel de cifrado, detección de liberados, estado de clave de acceso, restricciones del dispositivo, perfiles instalados, políticas de seguridad y más
- Use DEP para inscribir automáticamente a los dispositivos propiedad de la corporación durante la activación con sus configuraciones y políticas
- El bloqueo de activación en Find My iPhone es habilitado, vinculando el dispositivo con el Apple ID del usuario.
- Informa si existe una cuenta iTunes en un dispositivo
- Vea informes detallados sobre documentos, usuarios, dispositivos, aplicaciones y más

Realice acciones

- Configure Wi-Fi, VPN y ajustes y perfiles de correo electrónico
- Localice, llame, bloquee un dispositivo o restablezca claves de acceso olvidadas
- Borre selectivamente información corporativa a la vez de mantener la información personal en un dispositivo propiedad de un empleado
- Lleve a cabo un borrado total de un dispositivo perdido o robado
- Cambie la política de iOS
- Habilite o inhabilite los controles de "roaming" de voz y datos

Catálogo de aplicaciones empresariales

- Capacidad de gestión de aplicaciones empresariales: Las aplicaciones móviles distribuidas por MaaS360 a los dispositivos iOS puede ser totalmente gestionadas, permitiéndole simplificar la implementación de las aplicaciones a la vez de incrementar la seguridad
  - Recomiende aplicaciones de iTunes a los empleados
  - Distribuya aplicaciones "hechas en casa" y publique actualizaciones
  - Envíe a distancia una aplicación a un dispositivo e instálela silenciosamente si el dispositivo está supervisado
  - Gestione los controles "Open In" (Abrir en) para restringir la apertura de archivos desde aplicaciones corporativas a personales y viceversa.
  - Conecte aplicaciones gestionadas a VPN para lograr acceso protegido a la red
  - Habilite "single sign-on" en todas la aplicaciones para autentificación
  - Aplique automáticamente cifrado de datos a aplicaciones de terceros
- Compatible con VPP de Apple
  - Distribuya e instale aplicaciones prepagas sin visitar App Store de Apple
  - Ahorre dinero reteniendo plena propiedad y control sobre las licencias VPP de aplicaciones y libros cuando los usuarios ya no las necesitan

Establezca y distribuya políticas

- Imponga requisitos de clave de acceso
- Configure restricciones de dispositivos
  - Imponga copias de respaldo cifradas
  - Restrinja el uso de cámara, FaceTime y Touch ID y más
  - Restrinja la instalación de aplicaciones, la compartición de Photo Stream y más
  - Fuerce el tráfico de Internet a través del servidor proxy HTTP global
  - Distribuya Wi-Fi, VPN y perfiles de correo electrónico, tales como ajustes de Exchange ActiveSync
- Gestione controles de iCloud
  - Gestione "syncing" de documentos, datos de aplicaciones, copias de respaldo de dispositivos y fotos con iCloud para usuarios, grupos o todos los dispositivos
- Incremente la seguridad de correo electrónico
  - Restrinja la capacidad de los usuarios de mover correos electrónicos entre cuentas, para protegerse contra la filtración de datos corporativos
  - Impida que las aplicaciones de terceros envíen mensajes de correo electrónico
- Configuración de Wi-Fi avanzada
  - Gestione y envíe ajustes de proxy y auto-incorporación de SSID
- Imposición de contraseña de iTunes
  - Requiere que los usuarios ingresen su contraseña de iTunes para tener acceso al contenido, aplicaciones y datos almacenados en iTunes
- Envíe un mensaje y número en Lock Screen si un dispositivo se pierde
- Permita la característica Handoff que habilita Continuidad, resultados de la web en la sync de Spotlight e iCloud para aplicaciones gestionadas.

Lanzamiento

Juntos, iOS 9 y MaaS360 están preparados para suministrar un nivel totalmente nuevo de características de seguridad, productividad y gestión de dispositivo y datos para ayudar a su organización a dar el paso siguiente en su camino a la movilidad.

Nuevas características de seguridad Empresarial de iOS 9

- Restrinja AirDrop para aplicaciones gestionadas e iCloud Photo Library
- Establezca nuevas restricciones Supervisadas para usar en App Store, atajos de teclado, Apple Watch, modificación de claves de acceso, descargas automáticas de aplicaciones y más
- Desactive "trust" (confianza) de aplicaciones empresariales en dispositivos supervisados

Nuevas características de distribución de aplicaciones de iOS 9

- La distribución de aplicaciones basada en el dispositivo, despliega las aplicaciones directamente en los dispositivos, usando el Programa de adquisiciones en volumen (VPP) y MaaS360 para asignar las aplicaciones directamente a un dispositivo con el número de serie, sin requerir una Apple ID
- Envíe o reciba aplicaciones públicas sin necesidad de que el usuario acceda a la Tienda de aplicaciones
- Las aplicaciones empresariales instaladas con MaaS350 son dotadas de "trust" de manera explícita, sin pedir al usuario confirmación de "trust"
- Si un dispositivo tiene una aplicación antes de ser Supervisado, las aplicaciones en el mismo serán gestionadas silenciosamente cuando pase a ser Supervisado
- Las aplicaciones adquiridas y distribuidas a través de VPP pueden ser asignadas a dispositivos o usuarios de cualquier país donde la aplicación esté disponible

Nueva gestión de dispositivos y datos de iOS 9

- MaaS360 puede activar actualizaciones de dispositivos con nuevas versiones de iOS para cualquier dispositivo en el Programa de Inscripción de Dispositivos (DEP, por sus siglas en inglés)
- El Configurador de Apple le permite desplegar previamente aplicaciones y secuenciar la inscripción de dispositivos con MaaS360 mediante DEP
- VPN por aplicación soporta UDP y TCP para secuenciar audio o video

Para obtener más información acerca de IBM MaaS360 e iniciar una prueba durante 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 hasta la fecha inicial de publicación y puede ser modificado por IBM en cualquier momento. No todas las ofertas se encuentran disponibles en todos los países en que IBM opera.

Los datos de rendimiento y los ejemplos de clientes citados se presentan solo con fines ilustrativos. Los resultados reales de rendimiento pueden variar según las configuraciones específicas y las condiciones de funcionamiento. Es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier otro producto o programa con 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 INCUMPLIMIENTO. Los productos IBM están garantizados de acuerdo con los términos y condiciones de los acuerdos en virtud de los cuales se suministren.

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 del sistema de TI comprende proteger los sistemas y la información a través de prevención, detección y respuesta ante el acceso indebido desde el interior y el exterior de su empresa. El 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. Ningún sistema o producto de TI se debe considerar completamente seguro y ningún producto o medida de seguridad se puede considerar completamente eficaz en la prevención del acceso indebido. Los sistemas y productos IBM están diseñados para formar parte de un enfoque de seguridad integral, que necesariamente comprenderá procedimientos operacionales adicionales, y podrían requerir 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-COES-01