



Principales ventajas

- Provea, proteja y administre sus dispositivos 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 de los sistemas operativos iOS, Android, Windows Phone y BlackBerry
 - 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
-

IBM MaaS360 Mobile Device Management

Proteja y administre los dispositivos móviles actuales

IBM® MaaS360® Mobile Device Management (Administración de Dispositivos Móviles) es una solución rápida y con características completas para configurar dispositivos para acceso empresarial y proteger a los datos corporativos en teléfonos inteligentes y tabletas – todo desde una pantalla única.

Como es una robusta plataforma de nube integrada, MaaS360 simplifica la administración de dispositivos móviles (MDM, por sus siglas en inglés) con rápido despliegue, visibilidad y control que abarca diversos dispositivos móviles, aplicaciones y documentos.

El despliegue es rápido. Con unos pocos clics, los administradores de TI pueden comenzar a inscribir dispositivos y administrar rápidamente todo el ciclo de vida del dispositivo móvil – desde la inscripción hasta la integración empresarial, configuración y administración, monitoreo y seguridad, soporte, y analítica e informes.

Resuelve sus desafíos de MDM

- Incremente la seguridad y la aplicación de cumplimiento
- Reduzca el costo de soportar activos móviles
- Refuerce la administración de aplicaciones y rendimiento
- Ayude a asegurar una mejor continuidad de los negocios
- Incremente la productividad y la satisfacción de los empleados

¿Por qué MaaS360?

- Enfoque demostrado a la administración de movilidad empresarial
- Poderosa administración y seguridad para abordar todo el ciclo de vida de la movilidad
- Se integra fácilmente con su infraestructura existente
- Simple y rápido con una excepcional experiencia de cliente





Figura 1: Ejemplos de MaaS360 en distintos dispositivos

Inscriba rápidamente dispositivos móviles

Mobile Device Management de MaaS360 racionaliza la instalación de la plataforma y el proceso de inscripción de dispositivos para simplificar las vidas de TI y los empleados.

- Seleccione servicios de MDM y configure los ajustes de inscripción de dispositivos
- Envíe solicitudes de inscripción por aire (OTA, por sus siglas en inglés) usando SMS, correo electrónico o un URL personalizado
- Autentifique con Active Directory/LDAP, usando una clave de acceso por una sola vez, o con SAML
- Cree y distribuya políticas personalizadas de uso aceptable y EULA
- Registre dispositivos corporativos y de empleados (traiga su propio dispositivo, BYOD)
- Inicie inscripciones de dispositivos individuales o a granel
- Aplique o modifique ajustes de políticas de dispositivos predeterminadas

Integre los dispositivos móviles con los sistemas empresariales

A través de MaaS360 Cloud Extender, la integración con sistemas empresariales es fácil y directa, sin necesidad de contar con servidores locales ni de reconfigurar redes.

- Descubrimiento instantáneo de dispositivos que accedan a sistemas empresariales
- Integre con Microsoft Exchange, Lotus Notes, Microsoft Office 365 y Gmail
- Aproveche las Autoridades existentes de Active Directory/LDAP y Certificate
- Administre políticas de BlackBerry Enterprise Server
- Conéctese con otros sistemas operativos a través de robustas API de web

Administre centralizadamente los dispositivos móviles

MaaS360 proporciona una consola de administración de dispositivos móviles unificada para teléfonos inteligentes y tabletas, con política y control centralizados a través de múltiples plataformas.

- Configure el correo electrónico, calendario, contactos, Wi-Fi y perfiles de VPN por aire (OTA)
- Apruebe o ponga en cuarentena nuevos dispositivos móviles de la red
- Cree grupos personalizados para administración granular
- Distribuya y administre aplicaciones públicas y corporativas
- Comparta y actualice documentos y contenidos de manera segura
- Defina derechos de acceso al portal administrativo en función de los roles dentro de Mobile Device Management de MaaS360
- Decomise dispositivos eliminando los datos corporativos y el control MDM

Salvaguarde proactivamente los dispositivos móviles

Mobile Device Management de MaaS360 proporciona seguridad dinámica y robusta, y capacidades de administración de cumplimiento para monitorear permanente los dispositivos y tomar medidas.

- Requiere políticas de clave de acceso con calidad, longitud y duración configurables
- Haga obligatorios los ajustes de visibilidad de cifrado y contraseñas
- Establezca restricciones para los dispositivos sobre características, aplicaciones, iCloud y clasificaciones de contenidos
- Detecte y restrinja dispositivos liberados y modificados
- Localice, bloquee y limpie a distancia los dispositivos perdidos o robados
- Limpie selectivamente los datos corporativos, dejando los datos personales intactos
- Implemente reglas de cumplimiento en tiempo casi real con acciones automatizadas
- Habilite reglas de geo-vallado para aplicar cumplimiento basado en la ubicación

Racionalice el apoyo de MDM

Mobile Device Management de MaaS360 brinda la capacidad de diagnosticar y resolver problemas de dispositivos, usuarios o aplicaciones permanentemente desde un portal basado en la red; así ofrece visibilidad y control detallados de TI, y facilita la productividad óptima del usuario móvil.

- Acceda a vistas de dispositivo para diagnosticar y resolver problemas
- Localice dispositivos perdidos o robados
- Restablezca claves de acceso olvidadas
- Envíe mensajes a los dispositivos
- Actualice los ajustes de configuración sobre pedido
- Ayude a los usuarios a ayudarse a sí mismos con un portal de autoservicio

Monitoree e informe sobre los dispositivos móviles

Los tableros de Mobility Intelligence™ entregan un resumen interactivo y gráfico de sus operaciones y cumplimiento de administración de dispositivos móviles, lo que permite a TI informar sobre demanda a toda la empresa.

- Informes de inventario detallados de hardware y software
- Detalles de configuración y vulnerabilidad
- Capacidades integradas de búsqueda inteligente a través de prácticamente cualquier atributo
- Listas de vigilancia personalizables para rastrear y recibir alertas
- Los ajustes de privacidad para BYOD bloquean la recolección de información personalmente identificable
- Administración de gastos móviles opcional para el continuo monitoreo y emisión de alertas sobre el uso de datos

Administración de dispositivos móviles instantánea

Mobile Device Management de MaaS360 es una plataforma MDM fácil de usar con la funcionalidad esencial para la administración de todo el ciclo de vida de los dispositivos móviles actuales, incluyendo los teléfonos y tabletas iPhone, iPad, Android, Kindle Fire, Windows Phone, Windows 10 y BlackBerry.

Características esenciales de MDM

- Inscripción por aire (OTA) mediante SMS, correo electrónico o URL
- Imposición de clave de acceso y cifrado
- Perfiles de correo electrónico, VPN y Wi-Fi
- Ajustes de restricciones para dispositivos
- Localización, bloqueo y limpieza (total y selectiva) remotas
- Detección de liberados (jailbreak) y root (modificados)
- Actualizaciones y cambios de políticas
- Informes de cumplimiento

Robusta administración de movilidad

- Controles de acceso a correo electrónico
- Integración con directorio corporativo
- Administración de certificados
- Ajustes de privacidad para BYOD
- Políticas de persona específicas para usuarios, no para dispositivos
- Motor de cumplimiento automatizado para tomar medidas en tiempo casi real
- Rastreo y geo-vallado de ubicación
- Tableros y alertas

Para obtener más información sobre las soluciones de prevención de fraude de IBM Security, póngase en contacto con su representante de IBM o Asociado de Negocios IBM, o visite el siguiente sitio web: ibm.com/security



© Copyright IBM Corporation 2016

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Creado en los Estados Unidos de América
Marzo de 2016

IBM, el logotipo de IBM, ibm.com y X-Force son marcas comerciales de International Business Machines Corp. registradas en numerosas jurisdicciones de todo el mundo. Mobile360®, Secure Productivity Suite™, Simple. Secure. Mobility.®, Trusted Workplace™, Visibility360®, y We do IT in the Cloud.™ y dispositivo son marcas comerciales o marcas comerciales registradas de Fiberlink Communications Corporation, una Compañía IBM. Otros nombres de productos y servicios pueden ser marcas comerciales de IBM u otras empresas. Puede consultar la lista actualizada de las marcas comerciales de IBM en la web que aparece bajo el epígrafe “Copyright and trademark information”, en la dirección ibm.com/legal/copytrade.shtml

Apple, iPhone, iPad, iPod touch e iOS son marcas comerciales registradas o marcas comerciales de Apple Inc. en Estados Unidos y en otros países.

Microsoft, Windows, Windows NT y el logotipo de Windows son marcas comerciales de Microsoft Corporation en Estados Unidos y/o en otros países.

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