



Principales ventajas

- Aprovechone, proteja y gestione sus dispositivos 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 iOS, Android, Windows Phone y BlackBerry
 - 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
-

IBM MaaS360 Mobile Device Management

Proteja y gestione los dispositivos móviles de hoy en día

IBM® MaaS360® Mobile Device Management es una solución rápida y completa creada para configurar dispositivos como puntos de acceso empresarial y proteger los datos corporativos en smartphones y tabletas. Todo ello desde una única pantalla.

MaaS360 es una plataforma cloud integrada y robusta que simplifica la gestión de dispositivos móviles (MDM) con un rápido despliegue, visibilidad y control de dispositivos móviles, aplicaciones y documentos.

El despliegue es rápido. Con solo unos clics, los administradores de sistemas pueden empezar a inscribir dispositivos móviles y gestionar su ciclo de vida completo, desde su inscripción hasta su integración en la empresa, configuración y gestión, supervisión y seguridad, soporte técnico, análisis y creación de informes.

Responda a los retos que plantea la gestión de dispositivos móviles

- Aumente la seguridad y el cumplimiento normativo
- Reduzca los costes de mantenimiento de los activos móviles
- Mejore las aplicaciones y la gestión del rendimiento
- Obtenga garantía de una mayor continuidad del negocio
- Aumente la productividad y la satisfacción de los empleados

Por qué MaaS360

- Método de eficacia probado para la gestión de la movilidad empresarial
- Potente sistema de gestión y seguridad para abarcar el ciclo de vida completo de las aplicaciones móviles
- Fácil integración con su infraestructura actual
- Sencillo y rápido con una experiencia del cliente excepcional

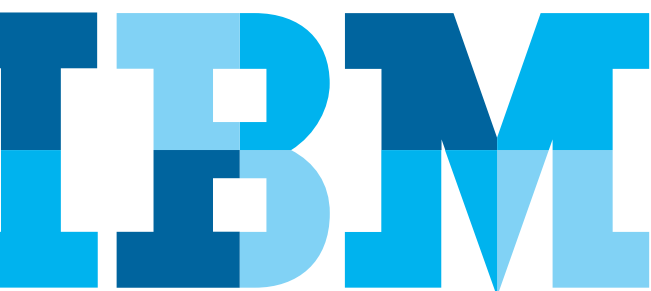




Figura 1: Ejemplos de MaaS360 en varios dispositivos

Rápida inscripción de dispositivos móviles

MaaS360 Mobile Device Management racionaliza la configuración de las plataformas y el proceso de inscripción de dispositivos para hacerle más fácil la vida al departamento de TI y a los empleados.

- Seleccione servicios de gestión de dispositivos móviles y configure valores de inscripción de dispositivos
- Envíe solicitudes de inscripción mediante protocolo OTA por SMS, correo electrónico o una URL personalizada
- Proporcione autenticación en Active Directory/LDAP mediante códigos de acceso de un solo uso o con SAML
- Cree y distribuya políticas de uso y acuerdos de licencia aceptables y personalizados
- Registre los dispositivos corporativos y los propios de los empleados (BYOD)
- Inicie inscripciones de dispositivos masivas o individuales
- Aplique o modifique valores de políticas de dispositivos predeterminados

Integre los dispositivos móviles con los sistemas empresariales

Con MaaS360 Cloud Extender, la integración con el sistema empresarial resulta fácil y directa, sin necesidad de servidores in situ o reconfiguraciones de la red.

- Descubra de forma instantánea los dispositivos que acceden a los sistemas empresariales
- Realice la integración con Microsoft Exchange, Lotus Notes, Microsoft Office 365 y Gmail
- Construya sobre Active Directory/LDAP y las entidades certificadoras existentes
- Gestione políticas BlackBerry Enterprise Server (BES)
- Conéctese con otros sistemas operativos a través de API web robustas

Gestione de forma central los dispositivos móviles

MaaS360 proporciona una consola unificada de gestión de dispositivos móviles para smartphones y tabletas con una política centralizada y control entre diferentes plataformas.

- Configure el correo electrónico, el calendario, los contactos, la Wi-Fi y los perfiles VPN mediante el protocolo OTA
- Apruebe o ponga en cuarentena nuevos dispositivos móviles en la red
- Cree grupos personalizados para una gestión más detallada
- Distribuya y gestione aplicaciones corporativas y públicas
- Comparta y actualice documentos y contenidos de forma segura
- Defina derechos de acceso al portal administrativo basados en roles en MaaS360 Mobile Device Management
- Retire dispositivos del servicio eliminando los datos corporativos y el control MDM

Proteja de manera proactiva los dispositivos móviles

MaaS360 Mobile Device Management ofrece una seguridad dinámica y robusta (así como funciones de gestión del cumplimiento) para supervisar de forma continua los dispositivos y tomar medidas.

- Especifique políticas de contraseñas con calidad, longitud y duración configurables
- Aplique ajustes de cifrado y de visibilidad de contraseñas
- Establezca restricciones para dispositivos en relación con algunas funciones, aplicaciones, iCloud y clasificación del contenido
- Detecte y restrinja dispositivos rooteados o liberados
- Localice, bloquee y limpie remotamente dispositivos perdidos o robados
- Limpie de forma selectiva datos corporativos dejando intactos los datos personales
- Implemente reglas de cumplimiento prácticamente en tiempo real con acciones automatizadas
- Defina reglas de “geo-fencing” para aplicar el cumplimiento en función de la ubicación

Racionalice el soporte de MDM

MaaS360 Mobile Device Management permite diagnosticar y resolver problemas de dispositivos, usuarios o aplicaciones de forma permanente desde un portal basado en web. Esto proporciona al departamento de TI una visibilidad y un control pormenorizados y permite optimizar la productividad de los usuarios de dispositivos móviles.

- Acceda a diferentes vistas de dispositivos para diagnosticar y resolver problemas
- Localice dispositivos perdidos o robados
- Restablezca contraseñas olvidadas
- Envíe mensajes a los dispositivos
- Actualice ajustes de configuración a petición
- Ayude a los usuarios para que puedan ayudarse a sí mismos con un portal de autoservicio

Supervise e informe sobre dispositivos móviles

Los paneles de control de Mobility Intelligence™ proporcionan un resumen gráfico e interactivo de las operaciones de gestión de dispositivos móviles y cumplimiento y permiten al departamento de TI elaborar informes a petición en la totalidad de la empresa.

- Informes detallados de inventario de hardware y software
- Detalles sobre la configuración y las vulnerabilidades
- Funciones de búsqueda inteligente integradas en prácticamente cualquier atributo
- Listas de vigilancia personalizables para realizar seguimientos y recibir alertas
- Recopilación de bloques de valores de privacidad BYOD de información identificable personalmente
- Gestión opcional de los gastos móviles para disponer de un sistema permanente de supervisión y alertas del uso

Gestión instantánea de dispositivos móviles

MaaS360 Mobile Device Management es una plataforma de gestión de dispositivos móviles fácil de utilizar con las funciones esenciales necesarias para gestionar el ciclo de vida completo de los dispositivos móviles actuales, como iPhones, iPads, dispositivos Android, Kindle Fire, Windows Phone y smartphones y tablets BlackBerry.

Fundamentos de la Gestión de Dispositivos Móviles (MDM)

- Inscripción mediante protocolo OTA en servicios de mensajes, correo electrónico o una URL
- Exigencia de contraseñas y cifrado
- Perfiles de correo electrónico, VPN y Wi-Fi
- Configuración de restricciones de dispositivos
- Localización, bloqueo y borrado remotos (completos y selectivos)
- Detección de dispositivos rooteados y liberados
- Actualizaciones y modificaciones de políticas
- Informes de cumplimiento

Gestión robusta de la movilidad

- Controles de acceso al correo electrónico
- Integración de directorios corporativos
- Gestión de certificados
- Valores de privacidad BYOD
- Políticas de roles específicas de usuarios, no de dispositivos
- Motor de cumplimiento automatizado para tomar medidas prácticamente en tiempo real
- Seguimiento y perímetro de ubicación
- Paneles de control y alertas

Para obtener más información sobre las soluciones de prevención del fraude de IBM Security, póngase en contacto con su representante o Business Partner de IBM, o bien 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. BYOD360™, Cloud Extender™, Control360®, E360®, Fiberlink®, MaaS360®, MaaS360® y dispositivo, MaaS360 PRO™, MCM360™, MDM360™, MI360®, Mobile Context Management™, Mobile NAC®, 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 empresa de IBM. Otros nombres de productos y servicios podrían ser marcas comerciales de IBM o de otras empresas. Puede consultar una lista actualizada de las marcas comerciales de IBM en Internet, 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 o marcas comerciales registradas 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 otros países.

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