IBM MaaS360 Laptop Management para Windows

Protección de ordenadores portátiles, de sobremesa, ultrabooks y tablets desde una misma pantalla

Principales ventajas

- La seguridad de mantener actualizados los parches, archivos externos y archivos de firmas de software antivirus
- Cargar mediante Push parches de Microsoft y actualizaciones de aplicaciones en los dispositivos, independientemente de su ubicación
- Cargar software en dispositivos mediante Push, independientemente de su ubicación
- Ubicar el dispositivo
- Apagar o reiniciar el dispositivo
- Detener/iniciar/reiniciar un servicio
- Enviar mensajes o bloquear dispositivos
- Borrar el disco duro en caso de pérdida o robo del dispositivo
- Demostrar el cumplimiento normativo en auditorías
- Flujos de trabajo unificados y homogéneos en dispositivos de distintos factores de forma
- Inscripción de dispositivos OTA

Gestione dispositivos Windows en el cloud

IBM® MaaS360® Laptop Management para Windows ofrece una solución autoservicio basada en cloud que facilita y acelera la prestación de asistencia por parte de TI durante todo el ciclo de vida de un PC con Windows.

Racionaliza el proceso de protección de los distintos dispositivos informáticos con Windows de hoy en día, cada vez más variados, todo desde una misma ventana: el mismo portal utilizado para la administración de dispositivos móviles (MDM).

MaaS360 le ofrece una solución líder en el sector para unificar la forma de gestionar los distintos dispositivos de su entorno de TI, desde dispositivos Windows hasta portátiles Mac, así como smartphones y tablets con iOS, Android, Windows Phone y BlackBerry.

Tan sencillo como administrar dispositivos móviles

La sencilla inscripción "over-the-air" (OTA), similar a MDM, y un flujo de trabajo unificado y homogéneo, independiente del factor de forma del dispositivo, ofrecen un portal fácil de usar para los administradores de TI.

MaaS360 Laptop Management para Windows ofrece información útil sobre todos sus ordenadores portátiles, de sobremesa, ultrabooks y tablets. Recoger y correlacionar datos procedentes de estos dispositivos le proporciona una excepcional visibilidad del hardware y el software instalado, los parches que faltan, archivos de firmas antivirus desfasados y mucho más.

Los paneles de control de Mobility Intelligence™, incluido My Alert Center, le ayudan a cumplir las normas corporativas y legales.

Figura 1: Proteger y administrar dispositivos Windows

Más visibilidad

MaaS360 Laptop Management para Windows ofrece información sobre el hardware y software de ordenadores portátiles y de sobremesa, ultrabooks y tablets Windows. Un agente de software se ejecuta continuamente en los dispositivos gestionados para generar informes y análisis.

- Inventario de hardware
- Inventario de software, que incluye tipos de aplicaciones (aplicaciones Win32 y de Windows Store)
- Información del estado de las aplicaciones de seguridad:
  - Antivirus
  - Firewall personal
  - Antispyware
  - Cifrado de datos
  - Copia de seguridad y recuperación
- Información sobre el sistema operativo (SO)
- Niveles e información sobre parches del SO, como tamaño de los archivos, nivel de gravedad y cuántos usuarios aún no tienen cada uno
- Actualizaciones para aplicaciones de Windows, como Java y Adobe

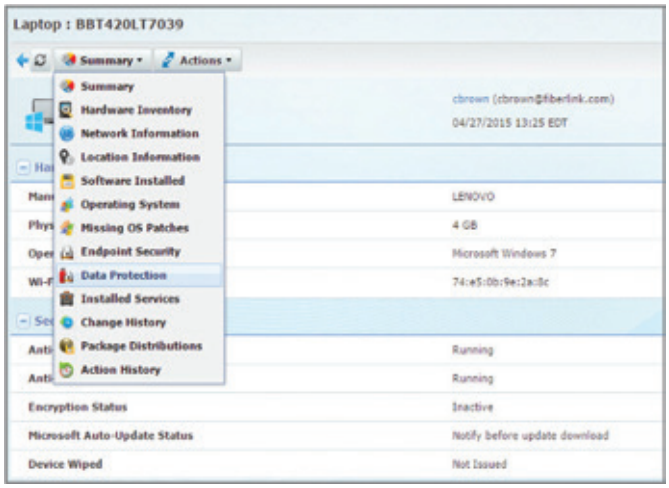

Figura 2: Ejemplo de información de dispositivo de un portátil con Windows

Tome el control

MaaS360 Laptop Management para Windows aumenta la visibilidad para facilitar a TI la administración de los dispositivos Windows en toda la organización. Mediante una consola centralizada, los administradores de TI pueden llevar a cabo distintas acciones con flujos de trabajo unificados.

- Inscribir dispositivos "over-the-air" (OTA)
- Identificar, programar e instalar parches pendientes del SO
- Localizar, bloquear, apagar o reiniciar el dispositivo
- Escoger un servicio para detenerlo, iniciarlo o reiniciarlo
- Distribuir paquetes con documentos y aplicaciones para aumentar la productividad de los empleados, protegiendo a la vez sus datos.
- Enviar un mensaje al usuario

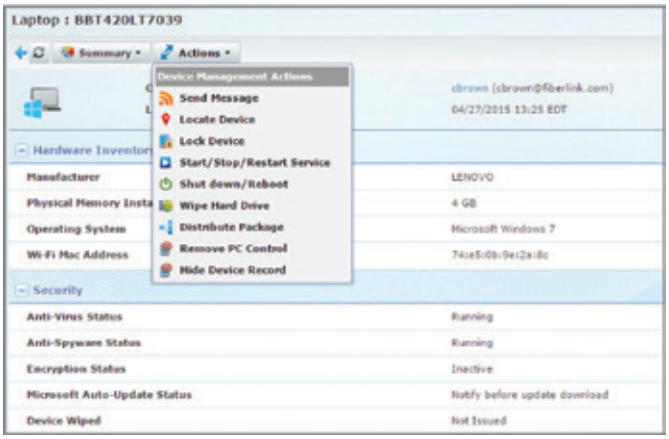

Figura 3: Ejemplo de acciones disponibles para un portátil con Windows

Distribución de parches y actualizaciones de las aplicaciones

MaaS360 Laptop Management para Windows resalta las actualizaciones pendientes de parches y actualizaciones de seguridad de Microsoft, así como las de las aplicaciones más habituales. Permite distribuir y aplicar las actualizaciones a sus dispositivos desde el mismo navegador, en el momento en el que el dispositivo se conecta a Internet.

Las cargas incluyen:

- Parches de MSFT
- Actualizaciones de iTunes
- Actualizaciones de Adobe
- Sistemas operativos
- Inventario de software

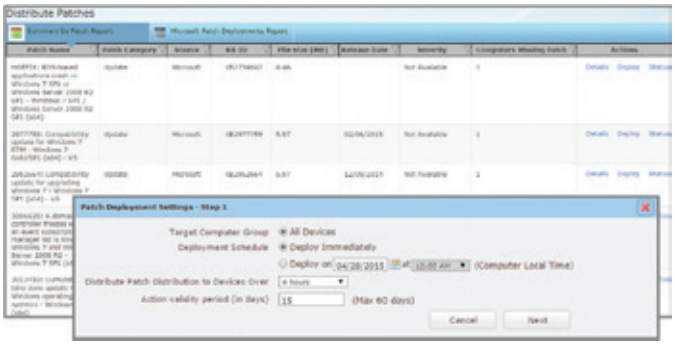

Figura 4: Ejemplos de configuración para distribución de parches

Proteja sus dispositivos Windows

MaaS360 es compatible con ordenadores portátiles, de sobremesa y ultrabooks con Windows, además de smartphones y tablets. Este tipo de dispositivos se puede gestionar a través de un solo portal al que se accede a través de un navegador web.

Crezca en el cloud

MaaS360 es una solución basada en el cloud, por lo que no necesita instalarla en sus servidores, llevar a cabo complejas configuraciones ni preocuparse del mantenimiento continuado. La implementación es rápida y sencilla, y con unos clics obtiene visibilidad y control instantáneos.

Con MaaS360, el departamento de TI puede gestionar y dar asistencia a los dispositivos informáticos móviles de la empresa, incluso sin que estén conectados a la red corporativa.

MaaS360 Laptop Management para Windows es compatible con Windows XP SP3, Windows Vista, Windows 7, Windows 8+, Windows 8+ Pro y Windows 10 (incluidas las versiones de 32 y 64 bits).

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.

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Creado en EE. UU.
Enero 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

WGD03059-ESES-01