

ManageEngine

Mobile Device Manager Plus

APROVISIONAR DISPOSITIVOS EN EL **MODO QUIOSCO** DE FORMA SEGURA Y EFICIENTE **MOBILE DEVICE MANAGER PLUS**



Introducción

Es común encontrar dispositivos móviles para el trabajo en las organizaciones de todos los tamaños. Las empresas del sector minorista, la salud, la educación y otros sectores permiten utilizar dispositivos móviles, como los smartphones y las tablets, porque permiten la movilidad de los trabajadores, ayudan a aumentar la productividad y simplifican las tareas repetitivas.

Sin embargo, esto conlleva algunos desafíos tales como el manejo de datos sensibles, como la información de identificación personal que requiere el cumplimiento de estrictas normas. Afortunadamente, las modernas herramientas de gestión de dispositivos móviles (MDM) y de gestión de la movilidad empresarial (EMM) ayudan a los administradores de TI a garantizar la seguridad de los dispositivos móviles.

El modo quiosco, o bloqueo de dispositivos, es un enfoque eficaz que las soluciones de MDM o EMM ofrecen para proteger el acceso a estos dispositivos de primera línea. La seguridad y las funciones de un quiosco dependen completamente de la forma en que se configure. Los casos comunes del modo quiosco incluyen aplicaciones de retroalimentación dirigidas a los clientes, portales web dirigidos a los empleados y dispositivos compartidos en las escuelas.

Esta guía paso a paso analiza cómo puede bloquear de forma segura los dispositivos móviles de su organización, independientemente del lugar en el que deben estar.



El modo quiosco dedicado frente a la alternativa nativa del dispositivo

Las opciones nativas del dispositivo, es decir, la fijación de la pantalla (Android) y el acceso guiado (iOS/iPadOS) ayudan a bloquear los dispositivos para que solo funcione una aplicación, pero eso es todo lo que pueden hacer y este método sólo proporciona funciones y seguridad rudimentarias. Los administradores de TI no podrán bloquear los dispositivos para más de una aplicación, determinar el aspecto de las pantallas del dispositivo o personalizar la barra de notificaciones y los botones del hardware. El departamento de TI ni siquiera podrá aplicar el bloqueo de forma remota, lo que es crucial para ahorrar tiempo y recursos.

Aunque las opciones nativas de los dispositivos son gratuitas, esto es relativo, ya que a menudo afectan negativamente a la productividad de los empleados, generan gastos adicionales por robos y violaciones de datos, y aumentan las horas de trabajo que TI dedica a la gestión de estos dispositivos.

Configurar los dispositivos sin una herramienta de gestión adecuada requiere de un gran esfuerzo, en el que las aplicaciones necesarias se deben instalar manualmente en cada dispositivo, y la configuración básica de las contraseñas, el Wi-Fi, la VPN, etc. también se deben realizar por separado. Esta podría no ser la forma más óptima de bloquear los dispositivos en las organizaciones que tienen un gran número de dispositivos.



Modo quiosco dedicado para una mejor gestión y seguridad

Una función de quiosco avanzada debe ser capaz de ayudar en toda la gestión del ciclo de vida del dispositivo. La gestión de quioscos no consiste únicamente en bloquear un dispositivo, sino también en garantizar que se proporciona la suficiente flexibilidad para que los empleados puedan realizar sus tareas sin problemas. Para gestionar eficazmente los dispositivos de quiosco, es fundamental que se cubran los siguientes aspectos:

01

Aprovisionamiento remoto

La capacidad de bloquear endpoints de diversos tipos y sistemas operativos en el modo quiosco desde una consola unificada, y garantizar que permanezcan bloqueados.

02

Implementación flexible

Elegir qué aplicaciones, portales web, recursos corporativos, configuraciones y funciones deben ser accesibles.

03

Personalización de la pantalla de inicio

La opción de personalizar el diseño y el orden de los iconos, organizarlos en carpetas, establecer la orientación y aplicar un fondo de pantalla a su elección.

04

Gestión de dispositivos robados y extraviados

Utilizar el modo perdido para bloquear, localizar y borrar datos de los dispositivos cuando se pierden o son robados.

05

Seguridad de datos

Establecer reglas proactivas y reactivas para garantizar la protección de la información sensible.

06

Perfiles de dispositivos

Abarca los aspectos de la gestión de dispositivos que no están relacionados con el quiosco y sus funciones auxiliares.

07

Gestión de aplicaciones

Implementar, configurar, actualizar y eliminar aplicaciones sin la intervención del usuario.

08

Información sobre el dispositivo y la batería

Recibir alertas sobre los niveles de batería, la ubicación del dispositivo, las actualizaciones de las aplicaciones y del sistema operativo, y el inventario exhaustivo del software y el hardware del dispositivo.

09

Solución de problemas de forma remota

La capacidad de controlar o ver a distancia las pantallas de los dispositivos y, posiblemente, sin necesidad de que intervenga el usuario.



3 cosas de las que se debe asegurar antes de aprovisionar los dispositivos en quioscos

Hay tres cosas que hay que tener en cuenta a la hora de bloquear los dispositivos para garantizar la mejor experiencia y seguridad del usuario final:

01

Software compatible

Asegúrese con suficiente antelación de que todos los dispositivos de su organización son compatibles con el software de bloqueo. Cuando se necesiten nuevos dispositivos y software de gestión de quioscos, evalúe la compatibilidad disponible para una amplia variedad de sistemas operativos y tipos de dispositivos para las compras actuales y futuras de dispositivos.

02

Línea de base de los dispositivos

Es crucial tener los dispositivos alineados según las políticas de TI y de cumplimiento de la organización. Esto refuerza la seguridad cuando los dispositivos se configuran como quioscos.

03

Bloqueo de dispositivos

Asegurarse de que la configuración del quiosco cumple las expectativas de los administradores de TI y de los respectivos departamentos mejora la experiencia de los usuarios al tiempo que aumenta la seguridad.

A continuación, se ofrecen algunas pautas sobre lo **que se puede configurar para bloquear los dispositivos correctamente:**

01 Inscribir un dispositivo con un MDM

Aunque hay soluciones dedicadas a los quioscos, un MDM puede proporcionar funciones avanzadas y personalización a diferencia de muchas soluciones específicas para quioscos disponibles en el mercado. También es importante asegurarse de que el dispositivo está inscrito en el modo "Propietario del dispositivo" si se ejecuta en Android, o está "Supervisado" si se ejecuta en iOS o iPadOS.

Definir las configuraciones según los estándares de la organización **02**

Establezca códigos de acceso, distribuya perfiles y certificados de Wi-Fi, VPN y proxy para garantizar una comunicación fluida, bloquee las aplicaciones y los sitios web no deseados y configure las actualizaciones de las aplicaciones y del sistema operativo. Es importante asegurarse de que las políticas de actualización estén configuradas para que se lleven a cabo durante horas no laborales para evitar interrupciones en el dispositivo durante el trabajo.

03 Distribuir aplicaciones, accesos directos a la web y contenidos

Distribuya los recursos que sus empleados, estudiantes o clientes necesitan. Esto podría incluir aplicaciones antivirus, herramientas de monitoreo de red, firewalls, portales de empleados y clientes o sitios web importantes.

04 Establecer políticas de seguridad específicas para el quiosco

En primer lugar, asegúrese de desactivar todo lo que no es necesario. Dependiendo del escenario de implementación, es posible que tenga que desactivar protocolos de red como Bluetooth, NFC y Wi-Fi directo, bloquear el uso compartido de USB y la copia de seguridad en la nube, y restringir las opciones de portapapeles y de uso compartido nativo presentes en las aplicaciones.

A continuación, asegúrese de habilitar todas las opciones que deben ser obligatorias. Configure el Wi-Fi, la localización y, si es necesario, los datos móviles, de modo que siempre estén activados. Asegúrese de que los dispositivos se conectan sólo a los SSID Wi-Fi designados, y configure perfiles Wi-Fi de reserva como contingencia cuando la red principal no esté disponible.

Por último, configure un geoperímetro en el dispositivo. Esto garantiza que el dispositivo se bloquee y se envíe una alerta cuando el dispositivo salga de un radio de ubicación preestablecido.

Asegurarse de que la resolución de problemas a distancia está configurada

05

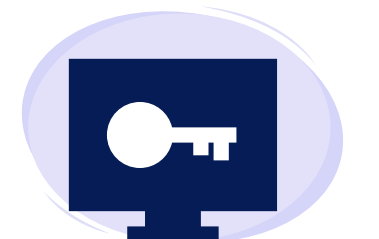
Dependiendo de su proveedor de MDM, es posible que tenga que realizar integraciones y complejos ajustes en las aplicaciones para solucionar los problemas de sus dispositivos. Asegúrese de que todo esto esté completo y de que esté habilitado el acceso sin supervisión o la capacidad de controlar o ver las pantallas de forma remota sin interactuar con el usuario. Esto ahorra mucho tiempo y esfuerzo de coordinación en los dispositivos que no están asignados a un usuario específico.

Bloquear los dispositivos de la manera correcta

Los administradores de TI necesitan configurar el modo quiosco en los dispositivos de diferentes maneras, dependiendo de los casos de uso. Según esto, es posible que necesiten personalizar el bloqueo en función de estas categorías:



Modo de implementación del quiosco



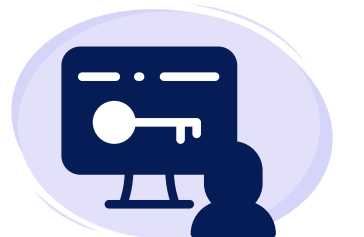
Los administradores de TI pueden bloquear la mayoría de los dispositivos modernos, ya sea para una sola aplicación, como en el caso de un quiosco de información orientada al público, o para un conjunto de aplicaciones, como los dispositivos entregados a los profesionales de la salud en los hospitales.

Puede haber situaciones en las que las aplicaciones no deban estar expuestas al usuario final, pero que deban ejecutarse en segundo plano para el buen funcionamiento de la empresa. Por ejemplo, podría tratarse de una aplicación de VPN o antivirus que se ejecuta en los dispositivos. Este tipo de aplicaciones se pueden aprovisionar como aplicaciones ocultas, siempre que su proveedor de EMM lo facilite.

A veces, es vital automatizar el bloqueo del dispositivo y evitar que los iPads accedan a aplicaciones específicas, como cuando los estudiantes están haciendo un examen. Esto puede lograrse aprovechando el modo autónomo de aplicación única de Apple. Las condiciones y las acciones personalizadas pueden iniciar el bloqueo si se configura de antemano en una aplicación compatible.

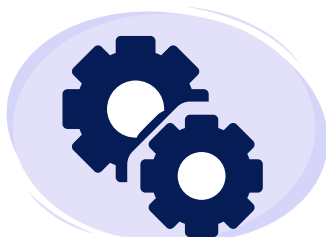
Proporcionar libertad de acción al personal adecuado

La flexibilidad en el bloqueo del dispositivo sólo se consigue cuando el personal autorizado puede acceder a todo el dispositivo. Esto puede lograrse exigiendo códigos de acceso para salir del modo quiosco.



Del mismo modo, es importante proporcionar acceso a la configuración del dispositivo para activar y desactivar rápidamente las funciones en situaciones específicas. Pero mostrar toda la configuración disponible puede poner en peligro los archivos confidenciales, ya que el usuario podría obtener suficientes privilegios para desactivar el bloqueo del dispositivo. Por eso es importante establecer una aplicación de ajustes personalizados en los dispositivos para que sólo se muestren los ajustes que son vitales para las operaciones diarias.

Personalizar las funciones del dispositivo



Dependiendo del escenario de implementación, puede ser necesario personalizar ciertas funciones como el menú de notificaciones, los botones de encendido y volumen, y las funciones de llamada y SMS.

Por ejemplo, los conductores de camiones pueden necesitar acceso a las notificaciones, las llamadas y los SMS para realizar la entrega al cliente final, pero con un acceso reducido al dispositivo para eliminar las distracciones. Esto también se debe determinar hablando con los supervisores del departamento correspondiente y configurando las funciones respectivamente.

Personalizar la pantalla de inicio

Por último, es el momento de personalizar los fondos de pantalla y la estética general del dispositivo para que coincida con las necesidades de marketing de la marca de la organización.



También es importante organizar las aplicaciones, anclarlas para facilitar el acceso, organizarlas en carpetas y establecer la orientación de la pantalla en función del entorno. Los administradores de TI también pueden añadir accesos directos a portales web como un quiosco de autoservicio para empleados.

ManageEngine Mobile Device Manager Plus: Mucho más que una solución de quiosco

ManageEngine Mobile Device Manager Plus simplifica la gestión y la seguridad de sus dispositivos móviles, aplicaciones y datos. Se trata de una solución de gestión del ciclo de vida de extremo a extremo que ofrece la incorporación automatizada de dispositivos, la creación de líneas de base, la gestión de aplicaciones, la gestión de contenidos y la gestión del correo electrónico. Hay varias políticas proactivas y reactivas, como el acceso condicional y las acciones remotas, que mejoran la prevención de la pérdida de datos.

Las funciones de gestión de activos granulares que ofrece Mobile Device Manager Plus se pueden utilizar para inventariar aplicaciones, recopilar hardware y software granular, localizar el dispositivo en tiempo real y mantener su historial de localización.

Mobile Device Manager Plus también ofrece funciones como el control del nivel de la batería, el apagado y el reinicio remotos, el geoperimetraje, el modo perdido y el acceso remoto sin supervisión, que son especialmente útiles para la gestión de dispositivos de quiosco.

Mobile Device Manager Plus le permite aprovisionar dispositivos en su organización de forma segura y eficiente.

Descargue una prueba gratuita y totalmente funcional de 30 días de Mobile Device Manager Plus para explorar, en cuestión de minutos, cómo mejorar su gestión de quioscos.

**COMENZAR LA PRUEBA
GRATIS**

**PROGRAMAR UNA DEMO
GRATUITA**

