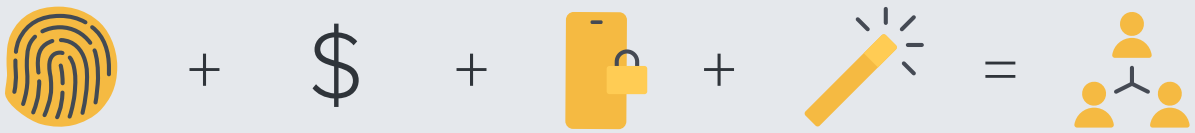
jamf

Jamf BYOD móvil: **privacidad y experiencia del usuario**

Aumente el BYOD móvil equilibrando la seguridad informática con la privacidad y la experiencia del usuario.

El auge del iPhone y el iPad como campeones de la productividad personal sin parangón ha dado lugar a una plantilla siempre conectada, moderna y móvil, y a un gran desafío para la administración de IT.

Elementos fundamentales para el éxito de las soluciones BYOD móviles



La posesión de dispositivos móviles es omnipresente y la mayoría de los empleados llevan su dispositivo personal al trabajo. Sin embargo, en los últimos años, intentar aprovechar el potencial de estos dispositivos no ha sido fácil. Muchos programas de "Traiga su propio dispositivo" (BYOD) han sido excelentes en su concepto, pero deficientes en la práctica. Los empleados proporcionan el hardware, las organizaciones proporcionan el acceso pero, con demasiada frecuencia, los dispositivos se administran en exceso o el empleado no recibe los servicios necesarios.

Por un lado, un marco de administración de dispositivos completo es demasiado invasivo porque el departamento de IT puede ver todas las aplicaciones del dispositivo, tanto las de trabajo como las personales. IT también tiene la capacidad de bloquear, desbloquear o borrar todo el dispositivo. A los propietarios de dispositivos móviles no les gusta ceder el control de su dispositivo ni ver comprometida su privacidad, ni siquiera tener la sensación de que esa privacidad está comprometida.

Otro método para administrar los dispositivos BYOD es la administración de aplicaciones móviles (MAM), que permite a IT aplicar las políticas corporativas a apps específicas suministradas al dispositivo. Esta técnica protege las aplicaciones, no la parte del dispositivo utilizada para trabajar. La implementación de MAM no dota a los administradores de la capacidad de proporcionar servicios corporativos, como la configuración de WiFi, el correo electrónico o la instalación automática de aplicaciones —ni siquiera las compradas por volumen—, lo que requiere una mayor interacción del usuario final. La ausencia de políticas corporativas básicas propicia que estos empleados se sientan desatendidos y que IT se sienta expuesta a vulnerabilidades de seguridad.

La realidad es que el éxito —o el fracaso— de un programa BYOD depende de si la tecnología es utilizable, los datos están seguros y la privacidad está protegida. **Este documento describe cómo Jamf y Apple ofrecen soluciones BYOD que logran ese equilibrio.**

La privacidad es lo primero

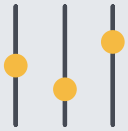
Nuestros dispositivos personales transportan los tipos de datos más privados: correspondencia personal, fotos, contactos y documentos. Incluso la elección de las apps instaladas en el dispositivo puede revelar información muy privada sobre nuestras aficiones, hábitos y estilo de vida. Con los temores distópicos del "Gran Hermano", no es de extrañar que la mayoría de los empleados sean reacios a brindar acceso a esa información inscribiendo su dispositivo personal en un sistema de administración de dispositivos móviles (MDM) controlado por el grupo de IT de su organización.

Cuando los programas BYOD fracasan, una razón común es la reticencia de los usuarios a ofrecer el acceso voluntariamente a estos datos personales a un administrador de IT. La privacidad personal importa, y los usuarios son cada vez más sensibles a cualquier intento de romper la barrera de la privacidad en nombre del control de IT.

La seguridad es importante para IT

Para el responsable de IT, la idea de un acceso sin restricciones a los recursos internos desde dispositivos personales con configuración y controles de seguridad desconocidos es un terreno fértil para las pesadillas. **Los dispositivos móviles son un objetivo común para los ataques de malware o phishing,** y presentan un vector potencial de intrusión cuando se conectan a la red de una organización.

Sin ninguna visibilidad ni control de los datos organizacionales de los endpoints, es una tarea imposible lograr una seguridad eficaz brindada por IT. La necesidad de seguridad es lo que empuja a las organizaciones a utilizar las MDM para su programa BYOD y, por tanto, a exigir a los empleados que inscriban su dispositivo personal para poder acceder a la red interna, al correo, a los calendarios, a la VPN, etc.



Los administradores de IT pueden:

- Emplear controles para la prevención de pérdida de datos
- Proporcionar un catálogo de apps Self Service administrado por el usuario
- Aplicar las configuraciones corporativas, como el Wi-Fi, la VPN y los requisitos del código de acceso
- Instalar y eliminar apps y libros corporativos y los datos asociados
- Recopilar información de seguridad de la cuenta de trabajo
- Agregar/eliminar restricciones que protejan los datos corporativos

Los administradores de IT no pueden:

- Borrar datos privados como fotos, correo personal o contactos
- Eliminar cualquier app personal
- Ver cualquier dato privado, incluidos los nombres de las apps personales
- Restringir el uso del dispositivo o limitar las apps personales que se pueden instalar
- Rastrear la ubicación del dispositivo
- Eliminar cualquier cosa instalada por el usuario
- Recopilar la información del usuario desde el dispositivo

Conseguir el equilibrio

Tanto los usuarios como IT tienen preocupaciones perfectamente válidas. El empleado solo quiere utilizar un dispositivo pero no quiere renunciar al acceso y control de sus datos privados. El departamento de IT quiere reducir los costos de los dispositivos, mejorar la experiencia de los empleados, pero sigue necesitando una seguridad organizativa básica. Para muchas organizaciones, estas disyuntivas significaron el fracaso de su programa BYOD.

Una solución para satisfacer ambas preocupaciones es replantearse el papel de la MDM en lo que respecta al BYOD. En lugar de un enfoque único, los administradores pueden elegir una herramienta diseñada para BYOD, con protecciones de privacidad para satisfacer a los empleados y fuertes controles de seguridad para satisfacer las necesidades de los equipos de InfoSec.

BYOD para la fuerza laboral moderna

Las organizaciones líderes eligen un conjunto de características creadas específicamente para el BYOD, para satisfacer las necesidades de ambas partes pero sin complejidades innecesarias ni costos añadidos. Es importante que tanto IT como el usuario final entiendan claramente los beneficios de un programa BYOD diseñado para ellos. También es fundamental para el éxito del programa proporcionar comunicación y transparencia a los empleados sobre las ventajas de un programa BYOD, ya que esto ayudará a aliviar cualquier tensión sobre el uso de un dispositivo de propiedad personal en el trabajo. A continuación se presentan algunos ejemplos de lo que la organización y los empleados pueden ganar con un programa BYOD bien diseñado.

El éxito se produce cuando todos ganan

Beneficios para los empleados

La experiencia nativa de Apple, tanto personal como profesional, todo en un solo dispositivo:

- Transparencia de las capacidades de administración de IT para un dispositivo de propiedad personal, antes de inscribirse, que garantiza la protección de los datos personales del usuario.
- Acceso seguro a los recursos corporativos como correo electrónico, calendarios, Wi-Fi y apps, facilitando la productividad.

Beneficios para la organización

Un equilibrio entre la seguridad y la privacidad del usuario final, todo en un solo dispositivo:

- Se garantiza la seguridad del dispositivo y el acceso a los datos y recursos corporativos, manteniendo a los empleados protegidos y productivos.
- Reducción de costos por la compra de menos dispositivos

Cómo garantizan Apple y Jamf la privacidad de los usuarios

Como se destaca en este documento, el objetivo es llegar a un punto óptimo para los dispositivos personales que no suponga una administración excesiva, pero que permita al departamento de IT servir adecuadamente a sus usuarios y a la organización mediante un acceso fácil y seguro al software y a las apps que los usuarios necesitan para su trabajo. Con esto en mente, Jamf ha impulsado a Apple para ampliar los beneficios y mejorar lo que es posible para los programas "Traiga su propio dispositivo".

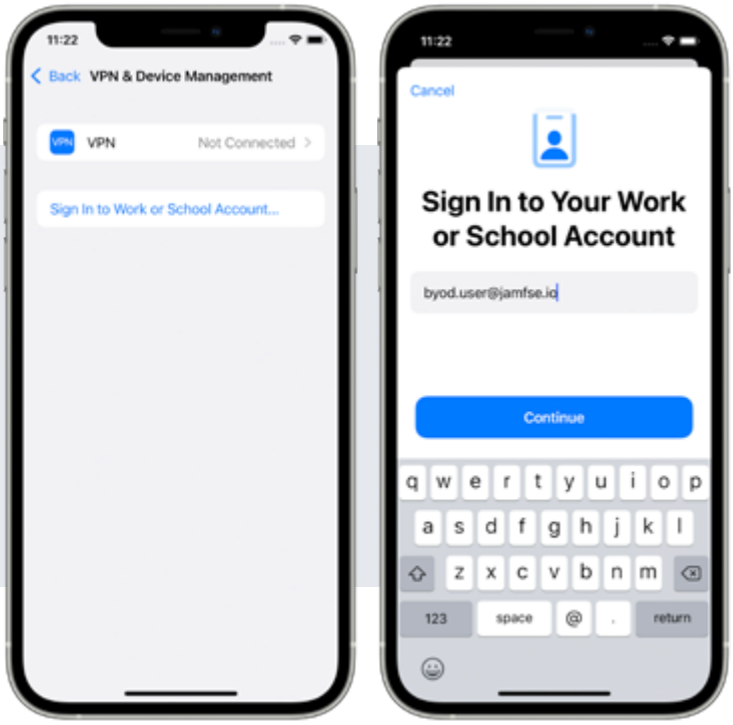
Con un fuerte enfoque en la seguridad y la privacidad, la **Inscripción del usuario basada en la cuenta** (Account-Driven User Enrollment) de Apple es un método BYOD para dispositivos iOS y iPadOS que agiliza el proceso de inscripción de usuarios y se centra en proporcionar acceso corporativo a los usuarios BYOD, manteniendo la privacidad del usuario en su dispositivo personal. Las organizaciones pueden aprovechar este nuevo flujo de trabajo para inscribir dispositivos móviles de propiedad personal con iOS y iPadOS 15 o posterior con Jamf Pro 10.33 o posterior. Jamf Pro es compatible con los flujos de trabajo de **inscripción de usuarios** nativos de Apple para configurar cuentas de trabajo y personales separadas, protegiendo así la privacidad de los empleados. Existen dos opciones de inscripción: inscripción de usuarios basada en cuentas e inscripción de usuarios basada en perfiles. Jamf prefiere la inscripción de usuarios basada en cuentas, en la que un empleado se inscribe desde la app Settings.

La inscripción de usuarios basada en la cuenta mantiene los datos personales e institucionales separados al asociar un ID de Apple personal con los datos personales y un ID de Apple administrado con los datos corporativos. Jamf Pro ha adoptado la función Service Discovery de Apple, lo que permite el uso de un conjunto de configuraciones que asocian la administración con el empleado y la forma en que utiliza el dispositivo para el trabajo, y no con todo el dispositivo en sí. Los empleados tienen la posibilidad de acceder a sus datos corporativos de forma segura sin que el departamento de IT tenga que tocar el dispositivo o enviarles un enlace de inscripción, lo que reduce la posibilidad de ataques de suplantación de identidad. El empleado recibe incluso Jamf Self Service, que puede utilizarse para instalar aplicaciones corporativas. Inscribirse es una experiencia familiar y de confianza que facilita las cosas para el empleado y un poco como una implementación sin contacto para los administradores, con las ventajas de proporcionar un acceso seguro a los recursos de sus organizaciones.

Cómo se inscribe un empleado

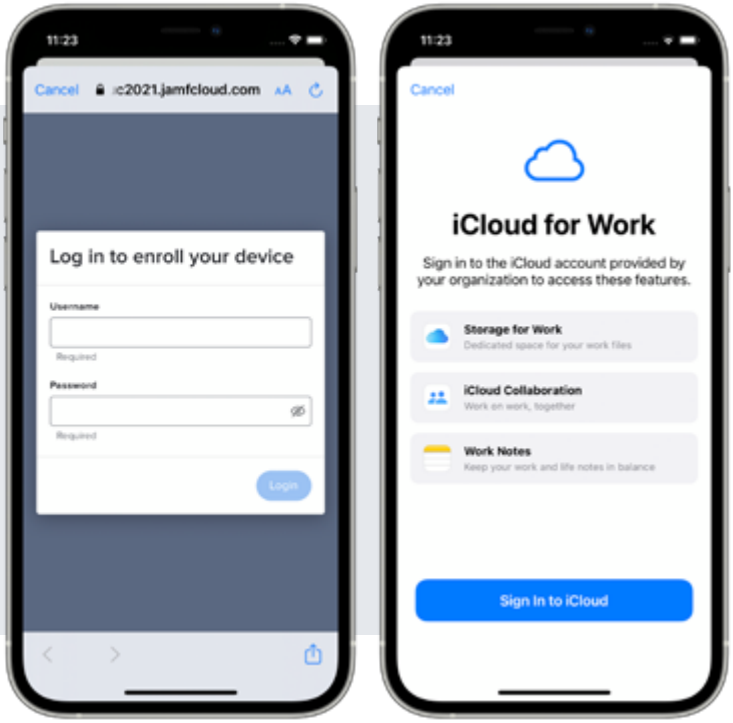
1

El usuario se autentifica en el dispositivo utilizando un ID de Apple administrado navegando a Ajustes > General > VPN y administración de dispositivos y, a continuación, inicia sesión en su cuenta de trabajo o escuela con su ID de Apple administrado. Después de que el usuario introduce el ID de Apple administrado, debe pulsar Continuar.



2

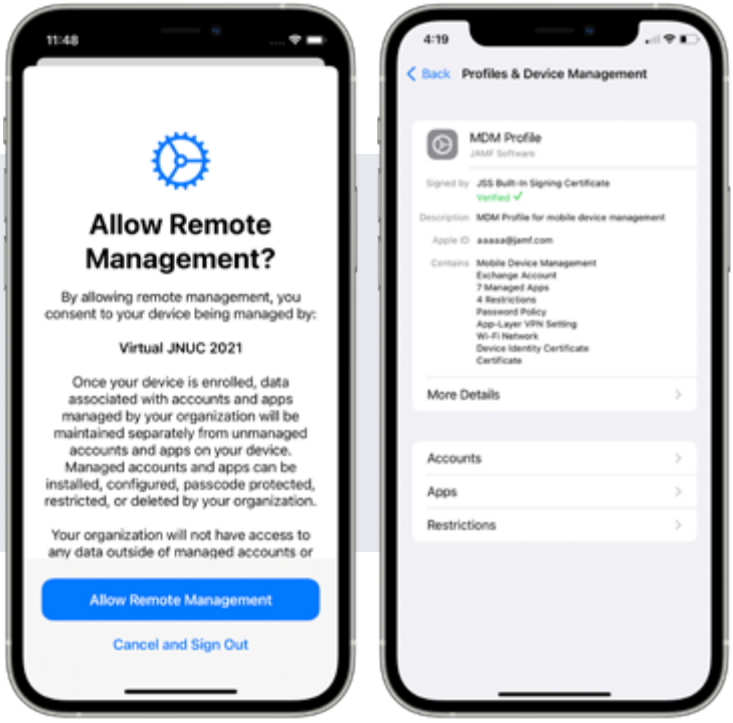
El portal de inscripción muestra y pide al usuario que introduzca su cuenta de usuario de Jamf Pro o sus credenciales de directorio (por ejemplo, LDAP o Azure AD). Después de introducir las credenciales, el usuario debe pulsar Login. A continuación, el usuario debe iniciar sesión en iCloud con su dirección de correo electrónico del ID de Apple administrado y su contraseña cuando se le solicite.



3

Se pide al usuario que permita la administración remota y la descarga del perfil MDM en el dispositivo.

¡Y eso es todo! Se trata de una experiencia sencilla para el usuario final, a la vez que segura para la organización.



Soluciones de acceso y seguridad para BYOD

Jamf Connect y Jamf Protect ofrecen soluciones adicionales y de seguridad.

Las funciones Zero Trust Network Access (ZTNA) de Jamf Connect garantizan que solo los usuarios de confianza con dispositivos seguros y autorizados puedan acceder a las aplicaciones y los datos de trabajo. Jamf Protect mejora la sólida seguridad de Apple para defender los datos de la organización.

Para que Jamf Connect y Jamf Protect funcionen, los administradores deben implementar Jamf Trust en los dispositivos de los empleados: una única app que ofrece las funciones de acceso y seguridad de Jamf Connect y Jamf Protect en los dispositivos móviles. Jamf Trust solo funciona en la cuenta de trabajo del dispositivo, dejando la cuenta personal en privado.

Conclusión

Un programa BYOD exitoso es un beneficio tanto para los empleados como para los administradores de IT. Con la solución MDM adecuada, IT puede concentrarse en atender las necesidades críticas de la empresa sin fricciones de la propia tecnología o de los usuarios. Y los usuarios se sienten cómodos y familiarizados con su propio dispositivo sin la participación intrusiva de IT.

Conozca más de **Inscripción de usuarios BYOD** o vea cómo Jamf con Apple pueden dar vida a sus planes BYOD al **Iniciar una prueba.**