Descripción de la implantación del Mac

Introducción

Índice

En Apple creemos que todos los empleados deberían tener acceso a las mejores herramientas y tecnologías para hacer su trabajo. Todos nuestros productos están desarrollados para que los empleados puedan ser más creativos, productivos y trabajen de formas nuevas dentro y fuera de la oficina. En consonancia con el modo en que los empleados quieren trabajar en el mundo actual, ofrecen un mejor acceso a la información, sistemas de colaboración e intercambio sin fricciones y libertad para comunicarse y trabajar desde cualquier lugar.

Configurar e implantar los ordenadores Mac en el entorno empresarial no puede ser más fácil. Gracias a la combinación de los servicios clave de Apple y una solución de gestión de dispositivos móviles (Mobile Device Management, MDM), cualquier empresa puede implantar y mantener fácilmente dispositivos Mac a escala. Si tu organización ya ha implantado dispositivos iOS y iPadOS a nivel interno, es más que probable que gran parte del trabajo de infraestructura necesario para implementar macOS ya esté hecho.

Gracias a las últimas mejoras introducidas en los ordenadores Mac en términos de seguridad, gestión e implantación, las empresas pueden cambiar los sistemas monolíticos de instalación por imagen y vinculación de directorios tradicional por un modelo optimizado de aprovisionamiento en el que el proceso de implantación se centre en el usuario y esté basado de manera prácticamente exclusiva en herramientas incluidas de serie con macOS.

En este documento encontrarás todo lo que necesitas saber para implantar ordenadores Mac a escala, desde cómo analizar tu infraestructura actual hasta cómo gestionar los dispositivos y aprovisionarlos de forma sencilla. Los temas abordados en este documento aparecen descritos en detalle en la «Guía de referencia sobre la implantación del Mac»: support.apple.com/guide/deployment-reference-macos

Primeros pasos

Todo proceso de implantación debe comenzar con dos pasos: el diseño de una estrategia de implantación y de un plan de ejecución, y la evaluación de todos los usos que los empleados dan a macOS. Asegúrate de involucrar a los equipos necesarios desde el principio del proceso y de que conozcan bien la visión y los objetivos del programa. Algunos equipos arrancan con una pequeña prueba de concepto para identificar los retos particulares planteados por su entorno. En un proyecto piloto más amplio, resulta fundamental escuchar a los usuarios para entender cómo se utilizan los dispositivos en la organización y saber si hay algún problema que deba abordar el equipo.

La información recogida durante esta fase puede ayudar a determinar qué empleados y funciones se beneficiarán en mayor grado del uso del Mac. Esto ayudará al equipo de TI a decidir cómo distribuir macOS, ya sea como el equipo estándar de toda la organización o como una opción para según qué funciones.

Durante esta fase se suele obtener una lista exhaustiva de apps y herramientas internas que deben ser compatibles antes de poder implantar el Mac de forma generalizada. Céntrate sobre todo en las principales apps de productividad, colaboración y comunicación que serán útiles para la mayoría de los usuarios. Ten en cuenta que los servicios corporativos críticos (como la intranet, el directorio y el software de gestión de gastos) también son importantes para que la empresa sea productiva.

Documenta y comunica cualquier solución provisional o alternativa para otras herramientas internas sin dejar de promover la modernización de las aplicaciones entre los propietarios. Sé transparente con los usuarios acerca de las distintas apps empresariales que podrán utilizar si eligen trabajar con el Mac y deja que sean ellos quienes determinen el orden de prioridad a la hora de modernizarlas. Llegado el momento, trabaja con los responsables de las apps para elaborar un plan de actualización utilizando tanto el SDK de macOS como Swift y recurriendo a socios comerciales que puedan ayudarlos a desarrollarlas.

Los ordenadores Mac suelen distribuirse como dispositivos propiedad de la empresa, pero hay empresas que eligen la implantación de dispositivos personales. En este modelo, los empleados utilizan sus propios Mac para trabajar. Independientemente del modelo de propiedad utilizado, permitir que los empleados trabajen con productos Apple puede reportarte beneficios en todas las áreas, como mayores niveles de productividad, creatividad, implicación y satisfacción en el trabajo, además de ahorro en costes derivados de los valores residuales y el soporte técnico. Las organizaciones también pueden beneficiarse de varias opciones de leasing y financiación para reducir los costes iniciales. Otra forma de compensar costes consiste en ofrecer a los empleados la opción de contribuir con deducciones en la nómina durante una actualización o permitirles comprar el equipo al final de un contrato de leasing o del ciclo productivo de un dispositivo.

Las políticas corporativas y los procesos de implantación, gestión y soporte técnico descritos en este documento pueden variar en función del tipo de información que recoja tu equipo de trabajo a lo largo del proyecto piloto. No todos los usuarios necesitan las mismas políticas, ajustes y apps, ya que los requisitos entre los distintos grupos o equipos de una empresa suelen variar sustancialmente.

Pasos de la implantación

La implantación de macOS suele dividirse en cuatro fases: preparación del entorno, configuración de la solución de MDM, implantación de los dispositivos entre los empleados y ejecución de las tareas de gestión continuada.

1. Preparación

Para empezar cualquier implantación tienes que fijarte en el entorno actual. Esta fase consiste en evaluar tu red y los componentes clave de tu infraestructura, así como en configurar los sistemas necesarios para llevar a cabo la implantación.

Evalúa la infraestructura

Aunque el Mac se integra perfectamente con la mayoría de los sistemas empresariales estándar, sigue siendo importante analizar la infraestructura de la que dispones para asegurarte de sacar el máximo partido a todo lo que ofrece macOS. Si tu organización necesita ayuda en esta área, puedes pedir asistencia a Apple Professional Services, así como a los equipos técnicos de tu socio del canal o distribuidor.

Wifi y redes

La configuración de los dispositivos macOS requiere un acceso amplio y fiable a una red inalámbrica. Confirma que la red wifi de tu empresa esté bien diseñada, sin olvidar el emplazamiento y la potencia de los puntos de acceso, para asegurarte de satisfacer las necesidades de itinerancia y capacidad.

Es posible que también tengas que ajustar las configuraciones de los puertos proxy o firewall si los dispositivos no pueden acceder a los servidores de Apple, el servicio de notificaciones push de Apple (APNs), iCloud o el iTunes Store. Al igual que con el iPhone y el iPad, hay partes del proceso de implantación del Mac (sobre todo con los equipos Mac más recientes) que requieren un acceso constante a estos servicios para tareas como la actualización del firmware durante la instalación.

Apple y Cisco han optimizado el modo en que los ordenadores Mac se comunican con las redes inalámbricas de Cisco incorporando compatibilidad con determinadas prestaciones de red avanzadas de macOS, como la de calidad del servicio (QoS). Si tu infraestructura de red es de Cisco, trabaja con tus equipos internos para asegurarte de que el Mac pueda priorizar el tráfico más importante.

Las empresas también tienen que evaluar la infraestructura de red privada virtual (VPN) para asegurarse de que los usuarios pueden acceder de forma segura a los recursos de la empresa desde cualquier lugar. Plantéate la posibilidad de usar la prestación VPN por Petición de macOS para que solo se inicien conexiones VPN cuando sea necesario. Si tienes la intención de usar VPN por App, comprueba que las puertas de enlace de tu VPN admitan estas funciones y adquiere suficientes licencias para cubrir el número de usuarios y conexiones que sean necesarios.

Asegúrate de que la infraestructura de red esté preparada para funcionar con Bonjour, el protocolo de red basado en estándares desarrollado por Apple que no requiere configuración previa. Bonjour permite que los dispositivos detecten los servicios de una red automáticamente. macOS usa Bonjour para conectarse a impresoras compatibles con AirPrint y dispositivos compatibles con AirPlay, como el Apple TV. Algunas apps y prestaciones de macOS integradas también usan Bonjour para detectar otros dispositivos a efectos de colaboración y uso compartido de contenido.

Más información sobre el diseño de la red wifi:
support.apple.com/guide/deployment-reference-macos

Más información sobre cómo configurar la red para MDM:
support.apple.com/HT210060

Más información sobre Bonjour:
support.apple.com/guide/deployment-reference-macos

Gestión de identidades
macOS puede acceder a los servicios de directorio, como Active Directory, Open Directory y LDAP, para gestionar identidades y otros datos de usuario. Algunos proveedores de MDM proporcionan herramientas para integrar sus soluciones de gestión con los directorios de Active Directory y LDAP sin pasos intermedios. Otras herramientas, como la extensión de inicio de sesión único de Kerberos de macOS Catalina, permiten integrar las políticas y funciones de Active Directory sin necesidad de recurrir a métodos tradicionales, como la creación de vínculos y cuentas móviles. También puedes gestionar varios tipos de certificados emitidos por autoridades de certificación (AC) tanto internas como externas con tu solución de MDM para que confíe en las identidades de manera automática.

Más información sobre la extensión de inicio de sesión único de Kerberos:
support.apple.com/guide/deployment-reference-macos

Más información sobre la integración de directorios:
support.apple.com/guide/deployment-reference-macos

Servicios básicos para empleados
Hay que asegurarse de que el servicio Microsoft Exchange esté actualizado y configurado en los dispositivos de todos los usuarios de la red. Si no usas Exchange, macOS también admite servidores estándar, como IMAP, POP, SMTP, CalDAV, CardDAV y LDAP. Prueba procesos de trabajo básicos relacionados con el correo electrónico, los contactos y los calendarios, así como otros programas de productividad para empresas, para cubrir el mayor porcentaje posible de procesos de trabajo críticos.

Más información sobre cómo configurar Microsoft Exchange:
support.apple.com/guide/deployment-reference-macos

Más información sobre los servicios basados en estándares:
support.apple.com/guide/deployment-reference-macos

Almacenamiento en caché de contenido
El servicio de almacenamiento en caché es una prestación integrada en macOS que almacena una copia local del contenido solicitado con frecuencia desde servidores de Apple con el objetivo de reducir el ancho de banda necesario para descargarlo en tu red. Puedes utilizar el almacenamiento en caché para acelerar la descarga y la distribución del software a través del Mac App Store. También es posible guardar en caché las actualizaciones de software para descargarlas rápidamente a los dispositivos de la empresa, sean macOS, iOS o iPadOS. Cisco y Akamai ofrecen asimismo sus propias soluciones de almacenamiento en caché desarrolladas por terceros.

Más información sobre el almacenamiento en caché de contenido:
support.apple.com/guide/deployment-reference-macos

Establece una solución de gestión

MDM permite a las empresas inscribir los Mac en su entorno con total seguridad, configurar y actualizar ajustes de manera inalámbrica, implantar apps, supervisar el cumplimiento de políticas, realizar consultas a dispositivos y eliminar o bloquear dispositivos gestionados de forma remota. El equipo de TI puede crear perfiles para gestionar cuentas de usuario, configurar ajustes del sistema, aplicar restricciones y usar políticas de contraseña desde el mismo sistema de MDM que ya usan para el iPhone y el iPad.

Al fin y al cabo, todas las plataformas de Apple utilizan un entorno de gestión propio común que permite a los clientes trabajar con distintas soluciones de MDM desarrolladas por terceros. Existe una amplia gama de soluciones de gestión de empresas independientes, como Jamf, VMware y MobileIron. Si bien macOS, iOS y iPadOS comparten muchos de los entornos de gestión de dispositivos, estas soluciones difieren en cuanto a las funciones de administración que ofrecen, los sistemas operativos con los que son compatibles, sus estructuras de precios y los modelos de alojamiento que proponen. También pueden ofrecer distintos niveles de servicios de integración, formación y soporte técnico. Antes de elegir una solución, evalúa qué prestaciones son las más interesantes para tu organización.

Cuando hayas elegido una solución de MDM, visita el portal de certificados push de Apple e inicia sesión para crear un nuevo certificado push de MDM.

Más información sobre la implantación de MDM:
support.apple.com/guide/deployment-reference-macos

Visita el portal de certificados push de Apple:
identity.apple.com/pushcert/

Inscríbete en Apple Business Manager

Apple Business Manager es un portal web para administradores de TI que centraliza la implantación del iPhone, iPad, iPod touch, Apple TV y Mac. En perfecta colaboración con tu solución de MDM, Apple Business Manager simplifica la automatización de la inscripción de dispositivos, la compra de apps, la distribución de contenido y la creación de ID de Apple Gestionados para los empleados.

Ahora, el Programa de Inscripción de Dispositivos (Device Enrollment Program, DEP) y el Programa de Compras por Volumen (Volume Purchase Program, VPP) están totalmente integrados en Apple Business Manager, de modo que las organizaciones disponen en un solo sitio de todo lo que necesitan para implantar dispositivos Apple. Estos programas dejarán de estar disponibles a partir del 1 de diciembre de 2019.

Dispositivos

Apple Business Manager permite la inscripción automatizada de dispositivos para que las organizaciones puedan implantar sus dispositivos Apple de forma rápida y optimizada e inscribirlos en MDM sin tener que tocarlos físicamente ni prepararlos de uno a uno.

- Simplifica el proceso de configuración para los usuarios optimizando los pasos del Asistente de Configuración de modo que los empleados tengan

las configuraciones correctas nada más activar sus dispositivos. Ahora, los equipos de TI pueden personalizar más a fondo esta experiencia proporcionando a los empleados texto de consentimiento, imagen de marca corporativa o un método de autenticación moderno.

- Refuerza el control de los dispositivos de la empresa mediante la supervisión, que proporciona controles adicionales de gestión de dispositivos que no están disponibles con otros modelos de implantación, incluido el de MDM no eliminable.
- Descubre una forma más sencilla de gestionar los servidores de MDM de forma predeterminada asociando un servidor por omisión a un tipo de dispositivo. Además, ahora puedes inscribir manualmente dispositivos iPhone, iPad y Apple TV con Apple Configurator 2, independientemente de dónde los hayas comprado.

Contenido

Con Apple Business Manager, las organizaciones pueden comprar contenido por volumen fácilmente. Con independencia del dispositivo que utilicen (iPhone, iPad o Mac), vuestra plantilla podrá disfrutar de contenidos listos para usar con opciones de distribución flexibles y seguras.

- Compra apps, libros y apps personalizadas por volumen, incluidas las apps que desarrollas internamente. Transfiere fácilmente licencias de apps entre centros de trabajo y comparte licencias con compradores del mismo centro. Y accede a un historial de compra unificado con información sobre el número de licencias utilizadas en ese momento a través de MDM.
- Distribuye apps y libros directamente a dispositivos gestionados o usuarios autorizados para que sea más fácil llevar un control del contenido que se ha asignado a cada cual. Con la distribución gestionada, controlarás todo el proceso de distribución y, además, conservarás los derechos de propiedad sobre las apps. Cuando un dispositivo o un usuario ya no necesite las apps asignadas, puedes revocarlas y reasignarlas a otros dispositivos y usuarios de tu organización.
- Paga tus compras de diferentes formas, como tarjetas bancarias y órdenes de compra. Las organizaciones pueden comprar Crédito VPP (donde esté disponible) a Apple o a un Distribuidor Autorizado Apple por importes concretos en la divisa local, que luego se transfieren electrónicamente al titular de la cuenta como crédito de la tienda.
- Aprovecha las ventajas de la distribución multinacional: distribuye una app a dispositivos o usuarios de cualquier país donde esa app esté disponible. Los desarrolladores pueden distribuir sus apps en diferentes países a través del proceso de publicación estándar en el App Store.

Nota: En algunos países o regiones no es posible comprar libros a través de Apple Business Manager. Para saber qué prestaciones y métodos de compra tienes a tu disposición, consulta support.apple.com/HT207305.

Personas

Con Apple Business Manager, las empresas pueden crear y gestionar cuentas para empleados que se integran con la infraestructura existente y facilitan acceso a apps y servicios de Apple, así como a Apple Business Manager.

- Crea ID de Apple Gestionados para que los empleados puedan colaborar con apps y servicios de Apple, y también para que accedan a los datos de trabajo en las apps gestionadas que usan iCloud Drive. Cada organización asume la propiedad y el control de estas cuentas.
- Usa la autenticación federada conectando Apple Business Manager con Microsoft Azure Active Directory. Se crearán ID de Apple Gestionados automáticamente la primera vez que cada empleado inicie sesión con sus credenciales existentes en un dispositivo Apple compatible.
- Usa ID de Apple Gestionados en un dispositivo propiedad del empleado junto con un ID de Apple personal con las nuevas prestaciones de inscripción de usuarios de iOS 13, iPadOS y macOS Catalina. Opcionalmente, los ID de Apple Gestionados se pueden usar en cualquier dispositivo como el ID de Apple principal (y único). Los ID de Apple Gestionados también tienen acceso a iCloud en la web después de iniciar sesión por primera vez en un dispositivo Apple.
- Designa funciones para los equipos de TI en la empresa con el fin de gestionar de manera efectiva los dispositivos, las apps y las cuentas en Apple Business Manager. Usa la función de Administrador para aceptar los términos y condiciones, si hace falta, y para transferir fácilmente la responsabilidad, si alguien abandona la organización.

Nota: Actualmente, iCloud Drive no es compatible con la inscripción de usuarios. iCloud Drive se puede usar con un ID de Apple Gestionado cuando es el único ID de Apple del dispositivo.

Más información sobre Apple Business Manager: www.apple.com/es/business/it

Inscríbete en el Developer Enterprise Program de Apple

El Developer Enterprise Program de Apple ofrece un completo conjunto de herramientas para desarrollar, probar y distribuir apps entre los usuarios. Puedes distribuir apps alojándolas en un servidor web o con una solución de MDM. Puedes firmar y autorizar los instaladores y las apps de Mac con tu ID de Desarrollador para que sean compatibles con Gatekeeper, que ayuda a proteger macOS del software dañino.

Más información sobre el Developer Enterprise Program: developer.apple.com/programs/enterprise

2. Configuración

Configurar la implantación consiste en definir políticas corporativas y preparar tu solución de MDM para configurar los Mac de la plantilla.

Conoce cómo funciona la seguridad en macOS

La seguridad y la privacidad son una parte fundamental del diseño del hardware, el software y los servicios de Apple. Protegemos la privacidad de los clientes con cifrados sólidos y políticas estrictas que rigen cómo se tratan todos los

datos. Estos son los requisitos para proporcionar una plataforma informática segura a los dispositivos Apple:

- Métodos que impidan el uso no autorizado de los dispositivos.
- Máxima protección de los datos, incluso si el dispositivo se pierde o lo roban.
- Protocolos de red y cifrado de los datos en tránsito.
- Permitir que las apps se ejecuten de forma segura sin comprometer la integridad de la plataforma.

Todos los dispositivos Apple contienen varias capas de seguridad para que puedan acceder de forma segura a los servicios de red y proteger los datos importantes. Otra forma de garantizar la seguridad en macOS, iOS y iPadOS es el uso de unas políticas de contraseña y código de acceso que se puedan distribuir y aplicar a través de MDM. Si un dispositivo cae en malas manos, un usuario o administrador puede utilizar un comando remoto para borrar toda la información privada.

El departamento de TI puede utilizar MDM para implantar un conjunto de políticas que refuercen la seguridad de los sistemas. Ejemplos de ello serían la obligación de usar FileVault y una custodia de la clave de recuperación con MDM, la obligación de usar una política concreta de contraseñas o de bloqueo del salvapantallas o la activación del firewall integrado.

Mas información sobre seguridad en la plataforma de Apple: apple.com/security/

Define políticas corporativas

Establece políticas generales que cubran a la mayoría de los usuarios del Mac de tu empresa para empezar el desarrollo de las políticas corporativas. Tu solución de MDM te permitirá definir personalizaciones específicas para cada usuario, como cuentas o acceso a determinadas apps. También puedes definir políticas específicas por departamentos o cualquier otro grupo de usuarios, como la implantación de aplicaciones o ajustes específicos según su cargo.

Trabaja con tus equipos internos para actualizar las políticas corporativas que la organización tenga en marcha e incorporar el uso de ordenadores Mac. Algunas políticas clave siguen siendo las mismas en todas las plataformas, como las de complejidad de la contraseña y requisitos de rotación, tiempos de espera del protector de pantalla y uso aceptable.

Si tu política corporativa exige una tecnología específica que se utiliza en otra plataforma, intenta entender el origen del problema para reformular la política y cubrir las tecnologías integradas de macOS. En lugar de exigir que todos los ordenadores utilicen una solución de terceros concreta para cifrar un disco entero, puedes crear una política que estipule que los datos corporativos deben cifrarse en reposo con FileVault. Si la política obliga a utilizar una aplicación antimalware concreta, da formación a los equipos sobre las prestaciones integradas, como Gatekeeper, y actualiza la política para permitirlas.

Configura los ajustes con MDM

Con el fin de permitir la gestión de las políticas corporativas y asegurarte de que los empleados puedan acceder a los recursos que necesitan, los Mac deben

inscribirse de forma segura con tu solución de MDM para que aplique las políticas y ajustes por medio de perfiles de configuración. Los perfiles de configuración son archivos XML creados por la solución de MDM para distribuir información de configuración entre dispositivos. Los perfiles de configuración automatizan la configuración de los ajustes, cuentas, políticas, restricciones y credenciales. Se pueden firmar y cifrar para ayudar a aumentar la seguridad de tus sistemas.

Una vez que un dispositivo está inscrito en una solución de MDM, el administrador puede ejecutar una política, consulta o comando de MDM. Con una conexión de red, el dispositivo iOS recibe una notificación de la acción del administrador a través del APNs para que pueda comunicarse directamente con su servidor de MDM a través de una conexión segura. Como la comunicación solo se establece entre la solución de MDM y el dispositivo, el APNs no transmitirá información confidencial ni privada. En el momento en que un dispositivo deja de gestionarse, los ajustes y políticas controlados por ese perfil de configuración se eliminan. Una empresa también puede borrar un dispositivo en remoto si es necesario.

Muchas organizaciones acceden a los servicios de directorio a través de su solución de MDM. El Asistente de Configuración de macOS puede pedir a los usuarios que inicien sesión utilizando las credenciales del servicio de directorio durante la inscripción automatizada. Con macOS Catalina, las nuevas opciones de inscripción personalizada permiten al Asistente de Configuración mostrar la autenticación de los proveedores de identidad en la nube. Una vez que el dispositivo está asignado a un usuario, MDM puede personalizar las configuraciones y las cuentas asignadas al individuo o al grupo al que pertenece. Por ejemplo, la cuenta de Microsoft Exchange de un usuario se puede aprovisionar automáticamente durante la inscripción. También es posible utilizar identidades de certificado para tecnologías como 802.1x, VPN, etc.

Dado el grado de control que proporcionan estos sistemas, muchas empresas confían la administración del Mac a los usuarios y les permiten personalizar los ajustes a su gusto, instalar las apps que quieran y diagnosticar problemas sin vulnerar el control de la política corporativa impuesta por MDM. Este modelo sigue los tipos de privilegios y controles de los que los usuarios disfrutan en sus iPhone o iPad cuando están gestionados.

Más información sobre los perfiles de configuración:
support.apple.com/guide/deployment-reference-macos

Prepara la inscripción automatizada de dispositivos

El método más sencillo para inscribir un dispositivo en MDM es el uso de las prestaciones de inscripción automatizada de Apple Business Manager durante el Asistente de Configuración. Esto permite inscribirlo sin ayuda del equipo de TI gracias a la optimización de la secuencia de pantallas, lo que agiliza el proceso.

Para configurar la inscripción automatizada de los dispositivos, tienes que vincular tu solución de MDM con tu cuenta de Apple Business Manager a través de un identificador seguro. Un proceso de verificación en dos pasos autoriza de forma segura una solución de MDM. Tu proveedor de MDM puede facilitarte documentación específica de implantación.

Si los dispositivos ya están en uso o son propiedad de los empleados, el usuario puede abrir un único perfil de configuración y verificarlo en las Preferencias del Sistema para concluir la inscripción. Este proceso se conoce como «inscripción en MDM aprobada por el usuario». Para gestionar ciertos ajustes de seguridad (como la política de extensiones del núcleo y el control de la política de preferencias de privacidad), la inscripción debe realizarse a través de la inscripción de dispositivos o de la inscripción en MDM aprobada por el usuario.

Más información sobre la carga de extensiones de núcleo:
support.apple.com/guide/deployment-reference-macos

Mas información sobre el control de la política de preferencias de privacidad:
support.apple.com/guide/mdm

Prepara la distribución de apps y libros

Apple ofrece programas muy completos que pueden ayudarte a sacar el máximo partido al excelente catálogo de apps y contenido disponible para macOS. Estas funciones te permiten distribuir entre tus empleados apps y libros adquiridos a través de Apple Business Manager o apps internas para que tengan todo lo que necesitan para hacer su trabajo. MDM también puede distribuir apps e instalar paquetes de software no disponible en el Mac App Store.

Tu solución de MDM puede utilizar la distribución gestionada para distribuir apps y libros adquiridos a través de la tienda de Apple Business Manager en cualquier país en el que esté disponible la app. Para activar la distribución gestionada, primero tienes que vincular tu solución de MDM con tu cuenta de Apple Business Manager mediante un identificador de seguridad. Una vez que te has conectado a la solución de MDM, podrás asignar apps y libros a los usuarios, incluso si el App Store está inhabilitado en el dispositivo. También puedes asignar apps a los dispositivos directamente, lo que facilita enormemente la implantación, ya que cualquier usuario del dispositivo tendrá acceso a ellas.

Mas información sobre la compra de contenido en Apple Business Manager:
support.apple.com/guide/apple-business-manager

Más información sobre la distribución de apps y libros:
support.apple.com/guide/apple-business-manager

Prepara el contenido adicional

Tu solución de MDM puede ayudarte a distribuir paquetes adicionales con contenido que no se origine en el Mac App Store. Se trata de una forma de distribución habitual para muchos paquetes de software empresarial, como aplicaciones internas personalizadas o apps como Chrome o Firefox. El software puede distribuirse a través de este método e instalarse de forma automática una vez concluida la inscripción. Los tipos de letra, los scripts y otros elementos también pueden instalarse y ejecutarse a través de paquetes. No olvides firmar siempre los paquetes con tu ID de Desarrollador del Developer Enterprise Program.

Mas información sobre la instalación de contenido adicional:
support.apple.com/guide/deployment-reference-macos

3. Implantación

Gracias a macOS, es muy fácil implantar dispositivos para el personal, personalizarlos y ponerlos a punto para trabajar sin ayuda del equipo de TI.

Utiliza el Asistente de Configuración

Los empleados pueden usar la utilidad Asistente de Configuración de macOS para definir las preferencias de idioma y región, además de para acceder a una red. Una vez que se conectan a internet, el Asistente de Configuración muestra a los usuarios diversas ventanas que les ayudan a configurar un Mac nuevo. Los dispositivos inscritos en Apple Business Manager pueden inscribirse automáticamente en MDM durante este proceso. Además, los Mac inscritos también se pueden configurar para omitir varias pantallas, como las de los términos y condiciones, el inicio de sesión con ID de Apple y los servicios de localización, entre otras.

MDM se puede usar después del Asistente de Configuración para implantar una amplia gama de ajustes tras la configuración inicial, como los privilegios administrativos del usuario. Al igual que en el iPhone y el iPad, esto les permite controlar su dispositivo sin vulnerar las políticas corporativas ni los ajustes gestionados por la solución de MDM. Para que los empleados puedan ponerse a trabajar nada más concluir el Asistente de Configuración, solo las aplicaciones y paquetes más críticos deberían empezar a descargarse e instalarse en segundo plano, sin entorpecer el trabajo del empleado. Para las aplicaciones más grandes, es posible programar su descarga e instalación en segundo plano o que el usuario utilice la herramienta de autoservicio de tu solución de MDM cuando le venga bien.

Configura las cuentas corporativas

MDM permite configurar el correo electrónico y otras cuentas de usuario automáticamente. En función de la solución de MDM y de su integración con tus sistemas internos, las cargas útiles de cuenta también pueden incluir varios datos del usuario, como nombre, dirección de correo y, si procede, identidades de certificado para tareas de autenticación y firma.

Permite que los usuarios personalicen sus dispositivos

Cuando los usuarios tienen la posibilidad de personalizar sus dispositivos, la productividad aumenta porque cada usuario puede elegir qué apps y contenido necesita para hacer su trabajo y cumplir sus objetivos de la mejor manera posible. Las empresas que usan los ID de Apple Gestionados e Inscripción de Usuario en macOS Catalina pueden ofrecer a los usuarios nuevas opciones para acceder a los servicios Apple únicamente a través de un ID de Apple propiedad de la empresa o en combinación con un ID de Apple personal.

ID de Apple personal e ID de Apple Gestionado

Al usar el ID de Apple para iniciar sesión en FaceTime, iMessage, el App Store y iCloud, entre otros servicios Apple, los empleados acceden a una serie de contenidos que les permiten agilizar las tareas, aumentar la productividad y trabajar en equipo. Al igual que cualquier ID de Apple, los ID de Apple Gestionados se usan para iniciar sesión en un dispositivo personal. También sirven para acceder a servicios de Apple —como iCloud y la colaboración con iWork y

Notas— y Apple Business Manager. A diferencia de los ID de Apple, la propiedad y gestión de los ID de Apple Gestionados corresponde a la propia empresa, lo que incluye el restablecimiento de contraseña y la administración basada en funciones. Los ID de Apple Gestionados pueden restringir determinadas configuraciones.

Los dispositivos inscritos a través de Inscripción de Usuario requieren un ID de Apple Gestionado. Inscripción de Usuario permite a la plantilla usar también su ID de Apple personal, mientras que las otras opciones de inscripción admiten, bien un ID de Apple propio, bien un ID de Apple Gestionado. El uso de varios ID de Apple solo es compatible con Inscripción de Usuario.

Los usuarios deben usar sus propios ID de Apple o los ID de Apple Gesionados para sacar el máximo partido a estos servicios. Si no tienen uno, pueden creárselo incluso antes de recibir un dispositivo. Asistente de Configuración también permite al usuario crear un ID de Apple personal, si no tiene uno. No necesitan una tarjeta bancaria para crear un ID de Apple.

Más información sobre los ID de Apple Gestionados:
support.apple.com/guide/deployment-reference-macos

iCloud
Con iCloud los usuarios pueden sincronizar automáticamente documentos y contenido personal —como contactos, calendarios, documentos y fotos— y mantenerlos actualizados en varios equipos. Buscar permite localizar un Mac, iPhone, iPad o iPod touch perdido o robado. Ciertas partes de iCloud —como Llavero de iCloud o iCloud Drive— pueden desactivarse a través de restricciones introducidas de forma manual en el dispositivo o a través de MDM. Así las organizaciones tienen mayor control sobre qué datos se almacenan en cada cuenta.

Más información sobre la gestión de iCloud:
support.apple.com/guide/deployment-reference-macos

4. Gestión

Una vez que los usuarios ya tengan sus dispositivos operativos, hay una amplia gama de funciones administrativas para gestionar y mantener los dispositivos y el contenido.

Administra dispositivos

La administración de un dispositivo gestionado puede realizarse desde la solución de MDM a través de una serie de tareas específicas. Esto incluye enviar consultas a los dispositivos e iniciar comandos que permitan gestionarlos en caso de incumplimiento de políticas, robo o pérdida.

Consultas
Las soluciones de MDM pueden enviar consultas a los dispositivos para ayudar al usuario a mantener las aplicaciones y los ajustes correctos. Las consultas pueden referirse al hardware, como el número de serie o el modelo de dispositivo, o al software, como la versión de macOS o una lista de aplicaciones

instaladas. Además, MDM puede consultar el estado de las principales prestaciones de seguridad, como FileVault o el firewall integrado.

Tareas de gestión
Cuando un dispositivo está gestionado, una solución de MDM puede ejecutar una amplia variedad de tareas administrativas, como cambiar la configuración automáticamente sin intervención del usuario, actualizar macOS, bloquear o borrar un dispositivo a distancia o gestionar las contraseñas.

Más información sobre las tareas de gestión:
support.apple.com/guide/deployment-reference-macos

Gestiona las actualizaciones de software

El equipo de TI puede ofrecer a los usuarios la opción de instalar la última versión del sistema operativo cuando esté disponible. Si prueban una versión de desarrollo de macOS, pueden identificar problemas de compatibilidad de aplicaciones para que los desarrolladores los solucionen antes de lanzar la versión final. Los equipos de TI pueden probar las versiones nuevas que van apareciendo a través del Apple Beta Software Program o de AppleSeed for IT. Protege a tus usuarios y sus datos manteniendo los ordenadores Mac actualizados. Actualiza con frecuencia y tan pronto como determines que tus procesos son compatibles con una versión nueva de macOS.

MDM puede enviar actualizaciones de macOS automáticamente a los Mac inscritos. Y si los sistemas críticos no están listos, estos Mac también pueden configurarse para actualizarse y recibir las notificaciones más tarde (90 días como máximo). Los usuarios no podrán iniciar las actualizaciones de forma manual hasta que la política se haya suprimido o MDM envíe un comando de instalación.

Apple no recomienda ni da servicio al sistema monolítico de instalación por imágenes para las actualizaciones de macOS. Al igual que el iPhone y el iPad, las actualizaciones de firmware de los ordenadores Mac suelen ser específicas para su modelo. Asimismo, las actualizaciones del sistema operativo del Mac exigen que Apple instale directamente estas actualizaciones de firmware. La estrategia más fiable es utilizar el Instalador de macOS o los comandos de MDM.

Gestiona el software adicional

Más allá del paquete inicial, a menudo las organizaciones necesitan distribuir apps adicionales entre sus usuarios. Esto puede gestionarse de forma automática con MDM para las aplicaciones y actualizaciones críticas o a la carta dejando que sean los propios empleados quienes soliciten las aplicaciones a través de un portal de autoservicio facilitado por tu solución de MDM. Estos portales pueden ejecutar muchas tareas distintas, como instalar el software adquirido en el App Store a través de Apple Business Manager o apps, scripts y otras utilidades adquiridas por otros medios.

Aunque la mayoría del software puede instalarse automáticamente, ciertas instalaciones pueden requerir la interacción del usuario. Para mejorar la seguridad, las apps que necesitan extensiones del núcleo tendrán que recibir el consentimiento del usuario para poder cargarse. Esto se conoce como «carga de extensiones de núcleo aprobadas por el usuario» y puede gestionarse a través de MDM.

Mantén la seguridad de los dispositivos

Más allá del conjunto inicial de políticas de seguridad que se hayan establecido antes de implantar los dispositivos, lo normal será que tu equipo quiera supervisar que las máquinas las cumplen y acceder a todo tipo de informes a través de tu solución de MDM. Estos informes pueden arrojar luz sobre la situación de seguridad de cada dispositivo o recopilar información de la instalación de parches de software. Aunque casi todas las empresas tienen suficiente con las herramientas nativas para cifrar y proteger los Mac, algunas pueden imponer el uso de otros servicios de sincronización e intercambio de archivos o herramientas de prevención de pérdida de datos para impedir la fuga de datos corporativos y obtener informes exhaustivos sobre los datos sensibles.

La prestación Buscar mi Mac de iCloud puede iniciar un borrado remoto que elimina todos los datos y desactiva un Mac si se pierde o cae en malas manos. Los equipos de TI también pueden ejecutar un borrado remoto con MDM.

Vuelve a aprovisionar los dispositivos

Cuando un empleado abandona la organización, Recuperación por Internet y la partición de recuperación local permiten volver a aprovisionar el Mac para traspasárselo a otro usuario. Esto permite borrar los datos del Mac e instalar la versión más reciente del sistema operativo. Una vez que se ha asignado un Mac a una solución de MDM específica en Apple Business Manager, el dispositivo se reinscribe automáticamente con MDM durante el Asistente de Configuración, configura los ajustes del nuevo usuario, aplica las políticas corporativas e instala el software adecuado. Los ordenadores Mac que no estén inscritos pueden borrarse y volver a aprovisionarse siguiendo el mismo proceso y reinscribirse de forma manual.

Opciones de soporte

Muchas empresas han constatado que los usuarios del Mac apenas necesitan la ayuda del equipo de TI. Los responsables de TI suelen crear herramientas de autoservicio para fomentar este tipo de soporte y mejorar la calidad de la asistencia. Por ejemplo, pueden ofrecer una buena página web de soporte del Mac, foros de autoservicio y puestos de ayuda técnica. Las soluciones de MDM también pueden permitir a los usuarios ejecutar tareas de mantenimiento, como instalar o actualizar software desde un portal de autoservicio.

Se recomienda no obligar a los usuarios a mantener los dispositivos sin ayuda. En su lugar, deben adoptar un modelo de resolución de problemas colaborativo que se centre en permitir que los usuarios diagnostiquen los problemas por sí mismos antes de llamar al equipo de asistencia técnica. Anima a los usuarios a asumir una parte de la responsabilidad en el proceso para que investiguen los problemas por sí mismos antes de pedir ayuda.

La responsabilidad compartida suele aumentar la disponibilidad de los dispositivos y reducir los costes y recursos humanos dedicados a dar soporte. Para las empresas que necesiten un nivel de soporte especializado, AppleCare oferta distintos programas y servicios dirigidos a los empleados y al departamento de TI que complementan las estructuras de asistencia técnica internas.

AppleCare for Enterprise

Para las organizaciones que busquen una cobertura completa, AppleCare for Enterprise puede ayudar a reducir la carga de trabajo del equipo de asistencia interno proporcionando soporte técnico telefónico para empleados de forma ininterrumpida y con respuesta en una hora para problemas de máxima prioridad. El programa ofrece a los departamentos de TI asistencia para situaciones complejas de integración, lo que incluye el uso de MDM y Active Directory.

AppleCare OS Support

AppleCare OS Support ofrece a tu departamento de TI soporte empresarial telefónico y por email para implantaciones de iOS, iPadOS, macOS y macOS Server. Incluye servicio ininterrumpido y un gestor técnico de cuentas según el nivel de soporte contratado. El personal de TI tendrá acceso directo a técnicos que resolverán sus dudas de integración, migración y uso avanzado de servidores, lo que mejorará su eficiencia a la hora de implantar, gestionar y resolver los problemas de los dispositivos.

AppleCare Help Desk Support

AppleCare Help Desk Support ofrece acceso telefónico prioritario a los expertos del servicio técnico de Apple. Además, incluye un paquete de herramientas para diagnosticar y solucionar problemas de equipos Apple, lo que puede ayudar a organizaciones grandes a gestionar los recursos de forma más eficiente, agilizar los tiempos de respuesta y reducir los costes de formación. AppleCare Help Desk Support cubre un número ilimitado de incidencias de diagnóstico y solución de problemas de hardware y software, así como detección de problemas en dispositivos iOS y iPadOS.

AppleCare y AppleCare+ para Mac

Todos los ordenadores Mac incluyen un año de garantía limitada y asistencia técnica telefónica gratuita durante los primeros 90 días a partir de la fecha de compra. La cobertura de este servicio se puede ampliar a tres años a partir de la fecha de compra original con AppleCare+ o AppleCare Protection Plan. Los empleados pueden llamar al equipo de soporte de Apple para hacer consultas de hardware o software. Apple también ofrece opciones de servicio muy interesantes en caso de que los dispositivos necesiten reparaciones. Además, AppleCare+ para Mac ofrece hasta dos incidencias de cobertura por daños accidentales, cada una sujeta a un cargo por servicio.

Más información sobre las opciones de soporte de AppleCare:
apple.com/es/support/professional/

Resumen

Dispones de muchas opciones para implantar y gestionar fácilmente los ordenadores Mac, ya sea para un grupo de usuarios o para toda tu empresa. Elegir las estrategias adecuadas puede ayudar a tu plantilla a ser más productiva y realizar su trabajo de formas completamente nuevas.

Más información sobre la implantación, gestión y prestaciones de seguridad de macOS:
support.apple.com/guide/deployment-reference-macos

Más información sobre los ajustes de gestión de dispositivos móviles para departamentos de TI:
support.apple.com/guide/mdm

Más información sobre Apple Business Manager:
support.apple.com/guide/apple-business-manager

Más información sobre los ID de Apple Gestionados para empresas:
apple.com/business/docs/site/Overview_of_Managed_Apple_IDs_for_Business.pdf

Más información sobre Apple at Work:
www.apple.com/es/business/

Más información sobre las prestaciones de TI:
www.apple.com/es/business/it/

Más información sobre la seguridad en la plataforma de Apple:
www.apple.com/security/

Echa un vistazo a los programas de AppleCare disponibles:
www.apple.com/es/support/professional/

Descubre Apple Training and Certification:
training.apple.com

Contacta con Apple Professional Services:
consultingservices@apple.com

© 2019 Apple Inc. Todos los derechos reservados. Apple, el logotipo de Apple, AirPlay, AirPrint, Apple TV, Bonjour, FaceTime, FileVault, iMessage, iPad, iPhone, iPod touch, iTunes, Mac y macOS son marcas comerciales de Apple Inc., registradas en EE. UU. y en otros países. Swift es una marca comercial de Apple Inc. App Store, AppleCare, Apple Books, iCloud, iCloud Drive, Llavero de iCloud y iTunes Store son marcas de servicio de Apple Inc., registradas en EE. UU. y en otros países. IOS es una marca comercial o una marca registrada de Cisco en EE. UU. y en otros países y se utiliza bajo licencia. Otros nombres de productos y empresas mencionados en el presente documento pueden ser marcas comerciales de sus respectivas compañías. Las especificaciones de producto están sujetas a cambios sin previo aviso. Este documento se proporciona con fines meramente informativos; Apple no asume ninguna responsabilidad relacionada con su uso.