

## Como Manejar Dispositivos Mac en la Empresa: 4 Enfoques y desafíos explicados

Los dispositivos Mac de Apple® están creciendo en popularidad corporativa cada día. Depende de los departamentos de TI asegurarse de que estos dispositivos utilicen todos los recursos en el entorno, así como garantizar que estén visibles y administrados.

Esto puede ser un desafío, ya que Mac y Windows son muy diferentes, y los dispositivos Mac siguen siendo una minoría en los entornos dominantes de Windows. Determinar cómo incorporar Mac en una infraestructura de Windows incluye una serie de factores, tales como: la cantidad de dispositivos que necesitan soporte; qué tipo de acceso requieren; y qué herramientas y sistemas ya tiene la organización. Los departamentos de TI también deben averiguar cómo integrar Mac con los dominios de Windows y Active Directory existentes.

En organizaciones centradas en Windows, administrar Mac no es la prioridad más alta en la lista de proyectos de TI por una variedad de razones. Pocos equipos de IT tienen experiencia en la gestión de Mac. Las técnicas conocidas para administrar PC no ayudan, y las mejores prácticas para tratar con Mac en una infraestructura empresarial compleja pueden ser complicadas y no son ampliamente conocidas.

Los equipos de TI adoptan cuatro enfoques principales cuando intentan adaptarse a dispositivos Mac:

1. Incorporar dispositivos Mac al dominio de Active Directory (AD) usando herramientas existentes destinadas a computadoras con Windows.
2. Uso de herramientas especiales de terceros para administrar dispositivos Mac en el dominio de AD.
3. Administrar Mac como dispositivos móviles.
4. Administrar computadoras Mac y PC en Microsoft SCCM.

Algunos equipos deciden tener dispositivos macOS® no administrados en el entorno, pero esto es un gran riesgo de seguridad. No necesariamente perderás tu trabajo si una Mac es hackeada y tu infraestructura se vuelve vulnerable, pero esto puede ser destructivo de muchas otras maneras.

Analicemos en profundidad estos cuatro enfoques para administrar dispositivos Mac en un entorno Windows.

### **1. Incorporar dispositivos Mac en el dominio de Active Directory usando las herramientas existentes.**

Esta es la preferencia de muchos administradores de TI. Es posible hasta cierto punto; Los equipos de escritorio y portátiles Mac incluyen el componente de cliente necesario para unirse a AD y otros servicios de directorio basados en estándares. Vincular una Mac al dominio es relativamente simple. Windows Server crea automáticamente el objeto de la computadora en AD (a menos que ya exista), justo como lo haría con un escritorio de Windows.

Las recientes versiones de macOS facilitan aún más la integración de los productos de Apple, ya que el sistema operativo puede funcionar con Microsoft System Center Configuration Manager (SCCM) y Microsoft Exchange ActiveSync.

Sin embargo, el hecho es que las computadoras Mac no son computadoras de escritorio con Windows, y la mayoría de los productos de administración están diseñados para Windows. Las capacidades nativas de

SCCM para dispositivos Mac son limitadas e insuficientes para la administración completa del ciclo de vida de macOS. Problemas de compatibilidad inevitablemente surgen. Una forma de solucionar estos problemas es extender el esquema de AD para que se adapte mejor a las computadoras Mac. Sin embargo, eso requiere recursos de desarrollo y experiencia técnica más allá de lo que muchas empresas pueden comprometerse, especialmente si los dispositivos Mac son minoría.

## **2. Usar herramientas especiales de terceros para administrar dispositivos Mac en el dominio de AD.**

El soporte de AD y comandos en macOS facilitan la integración de dispositivos Mac, pero a muchos administradores aún les gusta usar otras herramientas para ayudar con la administración. Por ejemplo, los administradores de TI pueden unir dispositivos Mac a dominios AD y luego usar Apple Remote Desktop™ para enviar comandos a los clientes Mac.

Una alternativa es implementar Mac OS X® Server en su propio sistema; El Administrador de perfiles de Apple puede ser usado para establecer políticas de Mac basadas en grupos de AD. Esto implica configurar un dominio Open Directory de Apple junto con el servicio AD, el cual puede facilitar la administración a largo plazo. Los dispositivos Mac aún están vinculados a AD, por lo que hay una comunicación perfecta entre los dos entornos, así como los servicios de archivos e impresoras compartidos.

Si esto suena demasiado complicado, existe Centrify User Suite (Mac Edition), que puede administrar dispositivos Mac y administrar de manera centralizada la autenticación, el cumplimiento de políticas y el inicio de sesión único. Otra opción es Jamf Pro, un producto integral de gestión de puntos finales.

## **3. Administrar Mac como dispositivos móviles.**

Apple se está moviendo hacia un modelo de administración de dispositivos móviles (MDM), en lugar de un modelo de servicios de directorio tradicional. Esto significa que los administradores de TI pueden usar las mismas herramientas de administración en computadoras Mac, iOS y dispositivos Android.

El nuevo Framework MDM de Apple permite a los administradores iniciar sesiones de AirPlay® en dispositivos administrados y enviar aplicaciones empresariales a computadoras Mac. Las capacidades y la plataforma mejorada de OS X Server también lo hacen más amigable con MDM. Los usuarios pueden registrar dispositivos Mac y los proveedores pueden hacer uso de una mayor cantidad de interfaces de programación de aplicaciones disponibles para soluciones de seguridad y administración de terceros.

Muchos proveedores de MDM han adoptado rápidamente nuevas características de Mac, como VMware AirWatch. AirWatch permite a los administradores administrar computadoras Mac junto con teléfonos inteligentes y tabletas y realizar una amplia variedad de tareas.

Las organizaciones también pueden implementar una herramienta separada, como MobileIron o un servidor de Apple no vinculado a AD. Esto permite a los administradores de TI implementar el acceso de los usuarios a través de redes virtuales privadas sin tener que unir los dispositivos al dominio. Esto es útil cuando se incorporan computadoras portátiles Mac personales de los usuarios.

#### 4. Administrar computadoras Mac y PC en Microsoft SCCM.

Este enfoque funciona mejor para las organizaciones que ya utilizan Microsoft SCCM para administrar las PC. Sin embargo, Microsoft SCCM por si solo tiene unas pocas funciones para administrar dispositivos Mac, no lo suficiente para administrar Mac en la empresa. SCCM permite lo siguiente:

- Configuración de soporte e inscripción de clientes macOS.
- Despliegue de configuraciones a clientes macOS.
- Realización de inventario de hardware de clientes macOS.
- Despliegue de aplicaciones a clientes macOS.

Si bien SCCM puede administrar estos dispositivos, es necesario instalar y configurar elementos adicionales para que sean compatibles con Mac. Se deberá implementar una infraestructura de clave pública para los Servicios de certificados de Active Directory. Estos certificados se utilizan para comunicarse con SCCM a través de comunicaciones SSL. Cada Mac con un cliente SCCM instalado actúa como un cliente basado en Internet.

Dado que los dispositivos Mac actúan como clientes basado en Internet, se deberá tener un servidor de Configuration Manager Site con un nombre de dominio completo, así como un mínimo de un punto de administración habilitado para HTTPS y un punto de distribución habilitado para HTTPS.

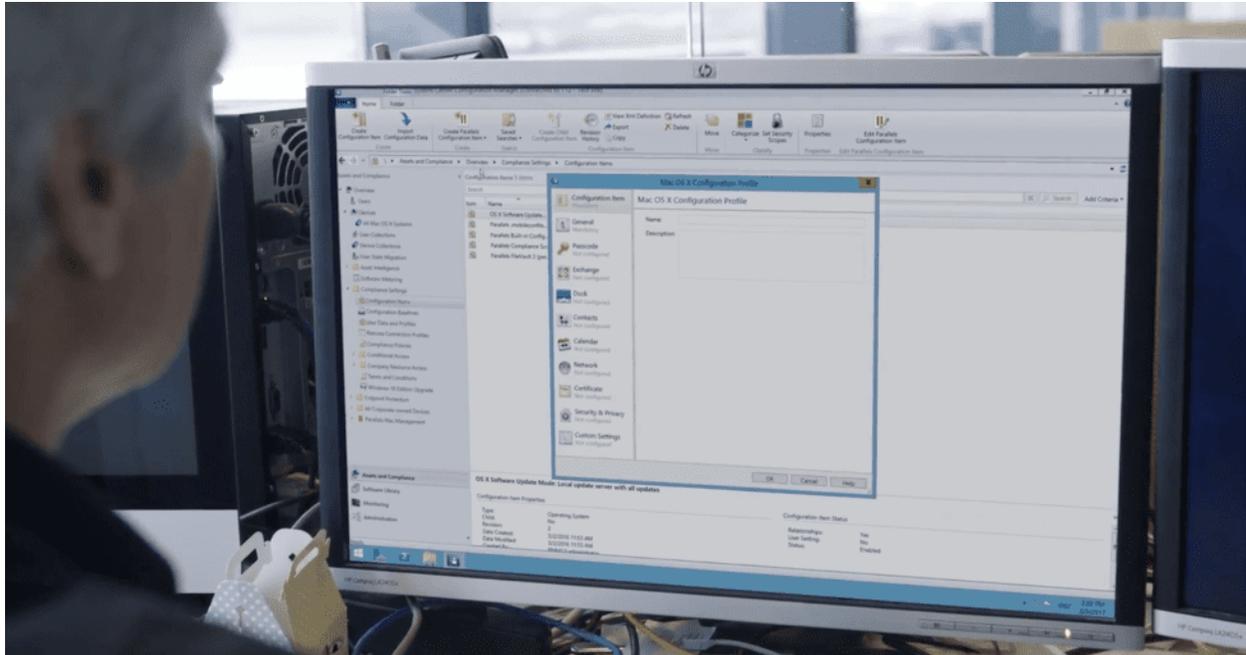
También se deberá configurar las funciones de punto de inscripción y punto de proxy de inscripción en SCCM. Esto permitirá que sus clientes macOS se inscriban en el entorno SCCM después de que se instale el cliente. Para habilitar la administración de estos clientes macOS, se deberá configurar los ajustes personalizados del cliente.

El soporte integrado de SCCM para Mac OS hace un buen trabajo, pero hay ciertas limitaciones en las características y funcionalidades de este soporte. Para administrar los clientes de Max OS X, se debe tener una infraestructura PKI y sistemas de sitio SCCM adicionales. Si no se planea habilitar las comunicaciones HTTPS para todo su entorno corporativo, se deberá tener múltiples puntos de administración y de distribución. Se configurará un punto de administración para las comunicaciones HTTP y otro para las comunicaciones HTTPS, al igual que para los múltiples puntos de distribución.

#### Amplíe SCCM para la administración de Mac a nivel empresarial

¿Qué pasaría si se pudiera agregar con un clic derecho la misma administración que reciben los dispositivos de Windows en SCCM a los dispositivos Mac? ¿Qué pasaría si pudiera hacerlo con una curva de aprendizaje corta, sin silos y con los mismos administradores de sistema?

Existe una solución que puede hacer todo esto y más: [Parallels® Mac Management for Microsoft® SCCM](#). Parallels Mac Management le da a SCCM todas las herramientas faltantes para la administración de Mac, incluido el cifrado FileVault® 2, el despliegue de macOS, la entrega de aplicaciones, el Programa de inscripción de dispositivos de Apple y la conformidad a través de elementos de configuración y líneas de base de SCCM.



Con Parallels Mac Management, simplemente agregue la administración completa del ciclo de vida de macOS a Microsoft SCCM y administre las computadoras PC y Mac en un solo panel de vidrio. Hay una curva de aprendizaje mínima y no se requiere infraestructura adicional. La solución aprovecha sus inversiones en Microsoft SCCM y permite a los administradores de Windows administrar computadoras Mac.

Para obtener más información sobre Parallels Mac Management, no dude en ponerse en [contacto](#) con nuestro equipo de ventas para solicitar una prueba gratuita.