qualoom®

Inspiring Technology
for People

Compatibilidad y Administración de **Dispositivos mediante Soluciones MDM**

Área de Seguridad
Fecha 28/05/2025
Versión 1.0

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

ÍNDICE

qualoom®

Inspiring Technology
for People

Introducción

En un entorno empresarial en constante transformación, la proliferación de dispositivos móviles y remotos ha introducido nuevos desafíos para los departamentos de TI. Desde asegurar la información hasta garantizar la productividad del usuario final, las soluciones de Mobile Device Management (MDM) son hoy esenciales para la administración segura, centralizada y escalable de infraestructuras digitales.

Este documento proporciona una visión técnica detallada sobre la compatibilidad de los dispositivos corporativos con las soluciones MDM más consolidadas del mercado: Microsoft Intune, JAMF Pro y SOTI MobiControl. Se examinan aspectos clave como la administración remota, el control de políticas de seguridad, la integración con directorios corporativos y la automatización de tareas de soporte técnico.

qualoom®

Inspiring Technology
for People

Fundamentos de MDM: **Un Pilar de la Seguridad Corporativa**

Las soluciones MDM permiten a los administradores gestionar dispositivos desde una consola centralizada, lo que es fundamental en estrategias de movilidad empresarial, entornos BYOD (Bring Your Own Device) y trabajo remoto.

Capacidades principales:

- Inscripción remota de dispositivos.
- Aplicación automática de configuraciones.
- Distribución y actualización de aplicaciones.
- Monitorización y análisis en tiempo real.
- Control de acceso según políticas de seguridad corporativa.

Una correcta implementación MDM reduce riesgos, mejora la eficiencia operativa y fortalece la postura de ciberseguridad de la organización.

qualoom®

Inspiring Technology
for People

Comparativa Técnica de **Plataformas MDM**

Característica	Microsoft Intune	JAMF Pro	SOTI MobiControl
Sistemas operativos compatibles	Windows, macOS, iOS, Android	macOS, iOS	Windows, Android, iOS, Linux
Administración remota total	✓	✓	✓
Control granular de políticas	Alto	Muy alto (Apple)	Alto
Integración con directorios	Azure AD, AD híbrido	LDAP, Apple School Manager	Active Directory, Azure AD
Automatización y scripting	PowerShell, Graph API	Scripts Bash/AppleScript	Scripts, comandos remotos
Informes y auditorías avanzadas	Power BI, Endpoint analytics	JAMF Compliance Reporter	SOTI Insight
Gestión de parches y actualizaciones	Intune Update Rings	Apple Software Update	Patch Management

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

Detalle de Integración **por Solución**

Microsoft Intune

Parte de Microsoft Endpoint Manager, Intune se integra nativamente con Azure AD y Microsoft 365, permitiendo:

- Autenticación condicional y multifactor (MFA).
- Aplicación de políticas de protección de aplicaciones (APP).
- Implementación sin contacto mediante Windows Autopilot.
- Gestión de dispositivos personales con aislamiento de datos corporativos.

Es la solución más adecuada para entornos Microsoft-centric y con dispositivos Windows 10/11.

qualoom®

Inspiring Technology
for People

Detalle de Integración **por Solución**

JAMF Pro

Diseñado específicamente para el ecosistema Apple, JAMF es la opción preferente para organizaciones con flotas de dispositivos macOS y iOS. Entre sus características destacan:

- Compatibilidad total con Apple Business Manager.
- Distribución automatizada de aplicaciones mediante VPP.
- Gestión de configuraciones a través de perfiles y scripts.
- Supervisión de estado del dispositivo y cumplimiento.
- Ofrece una experiencia de administración profunda, especialmente optimizada para entornos educativos y creativos.

qualoom®

Inspiring Technology
for People

Detalle de Integración **por Solución**

SOTI MobiControl

Su enfoque multiplataforma y versatilidad lo posicionan como una solución ideal para sectores con diversidad de dispositivos, como logística, retail o industria:

- Gestión extendida a dispositivos industriales (rugged).
- Políticas de geofencing y control por ubicación.
- Soporte para dispositivos con Linux, y Android embebido.
- Compatibilidad con terminales de código de barras y sensores.

Permite control avanzado de flotas mixtas en campo, con una visibilidad completa del estado operativo.

qualoom®

Inspiring Technology
for People

Seguridad Avanzada en **Entornos MDM**

La administración centralizada permite aplicar políticas de seguridad consistentes en todos los dispositivos. Las capacidades incluyen:

- Cifrado completo de datos en tránsito y en reposo.
- Autenticación multifactor (MFA) integrada en las plataformas.
- Borrado remoto seguro en caso de pérdida o robo.
- Restricción del uso de funciones como cámara, USB, hotspot, etc.
- Monitoreo de amenazas y cumplimiento normativo (GDPR, ISO 27001).

Todas las plataformas permiten auditorías detalladas, integración con SIEM y generación de reportes de cumplimiento para auditorías externas.

qualoom®

Inspiring Technology
for People

Casos de Uso **Relevantes**

Caso 1 – Despliegue educativo con JAMF

Una universidad despliega más de 2.000 iPads utilizando JAMF y Apple School Manager, logrando inscripción automática, gestión curricular y control granular de apps.

Caso 2 – Gestión de flotas industriales con SOTI

Una empresa logística utiliza SOTI MobiControl para controlar terminales Android industriales en 12 almacenes, aplicando políticas por geolocalización y actualizaciones programadas.

Caso 3 – Seguridad corporativa con Intune

Una multinacional del sector financiero integra Intune con Azure AD, utilizando MFA, políticas de protección de apps y acceso condicional basado en riesgo para proteger datos sensibles.

qualoom®

Inspiring Technology
for People

Recomendaciones **Técnicas**

- Analiza tu parque de dispositivos y necesidades de soporte.
- Implementa pruebas piloto para validar compatibilidad y rendimiento.
- Centraliza la documentación técnica de perfiles y configuraciones.
- Aplica una estrategia Zero Trust como marco de seguridad.
- Automatiza tareas mediante scripting y políticas dinámicas.

La capacitación continua del personal técnico y la revisión periódica de las políticas MDM son claves para mantener la efectividad del sistema a largo plazo.

CONCLUSIÓN

La elección de una solución MDM no debe basarse únicamente en costes o compatibilidad superficial. Es crucial alinear la herramienta con las políticas de seguridad de la organización, la diversidad del entorno operativo y la escalabilidad futura.

Las tres soluciones analizadas —Intune, JAMF y SOTI— ofrecen ventajas distintas que pueden combinarse o integrarse con sistemas existentes mediante APIs y conectores.