Device Management (KDM)

In today's rapidly evolving landscape, implementing a Mobile Device Management (MDM) solution is more crucial than ever to address the needs of both your business and your users. MDM focuses on deploying, securing, monitoring, integrating, and managing workplace devices, ensuring a consistent, secure, and productive environment. It also provides employees with the right tools to perform their tasks effectively..

If left unmanaged, your Apple and Windows workstations will become outdated and insecure, with unpatched operating systems and applications. Users will experience inconsistent settings across different devices, and the lack of management increases security vulnerabilities, making your systems more vulnerable to cyberattacks. Kaizen Device Management is our remote MDM service, created to address the challenges of this constantly evolving landscape. It offers a range of essential features, including:

- **Device consistency** – ensures that settings such as VPN, Wi-Fi, login windows, and other essential services are properly and uniformly configured across all devices, guaranteeing that every device is aligned with your business needs, regardless of the user.
- **Patch management** – Automates the security patching of operating systems and applications to protect against the latest vulnerabilities. It also ensures that everyone on your team is using the same version of applications, maintaining consistency and security across all devices.
- **Device Encryption** – Centrally manage the encryption of all devices to ensure that data remains inaccessible to unauthorised users. Encryption provides an additional layer of security, making it significantly harder for hackers to access sensitive information, even if they bypass other security defences.
- **Local Firewall Activation** – Centrally enable the local firewall to block unauthorised users or malicious software from accessing your computer through the internet or network. It acts as a protective barrier against malware, ransomware, and other cyber threats.
- **Remote Wipe** – A security feature that allows organisations to erase data on a business device remotely. It is typically used in cases where a device is lost, stolen or compromised to prevent unauthorised access to sensitive information.
- **Restrict Apps** – Block untested OS updates until fully tested or Apps considered unproductive such as Messaging Apps.
- **Full Inventory Information** – In addition to standard hardware details, gain access to critical data such as administrator accounts, installed applications, change history, and security configurations. This comprehensive overview helps maintain better control and security over your devices and IT environment.

Centralised User Management

Leveraging Cloud Directory Login is essential for businesses as it centralises user authentication and access management, improving security, efficiency, and flexibility. Cloud directory services like Microsoft and Google Workspace offer a unified platform for managing user accounts and access across all applications, simplifying the management of permissions, user roles, and access policies from a single location. These services also support Multi-Factor Authentication (MFA), providing an extra layer of security. Additionally, within Microsoft Tenancies, Conditional Access policies can be implemented for even more control.

kaizenit.co.uk
0345 141 1400
hello@kaizenit.co.uk