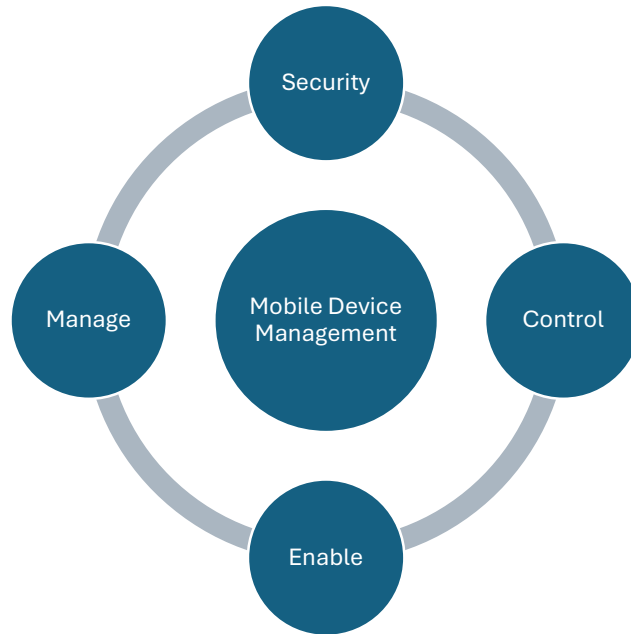


SCG Corporate – G Cloud 15

Service Description Mobile Device Management (MDM)



What is Mobile Device Management (MDM)?



Mobile Device Management (MDM) is the process of enhancing data security by **monitoring**, **managing** and **securing** the mobile devices such as laptops, smartphones and tablets that are used in enterprises.

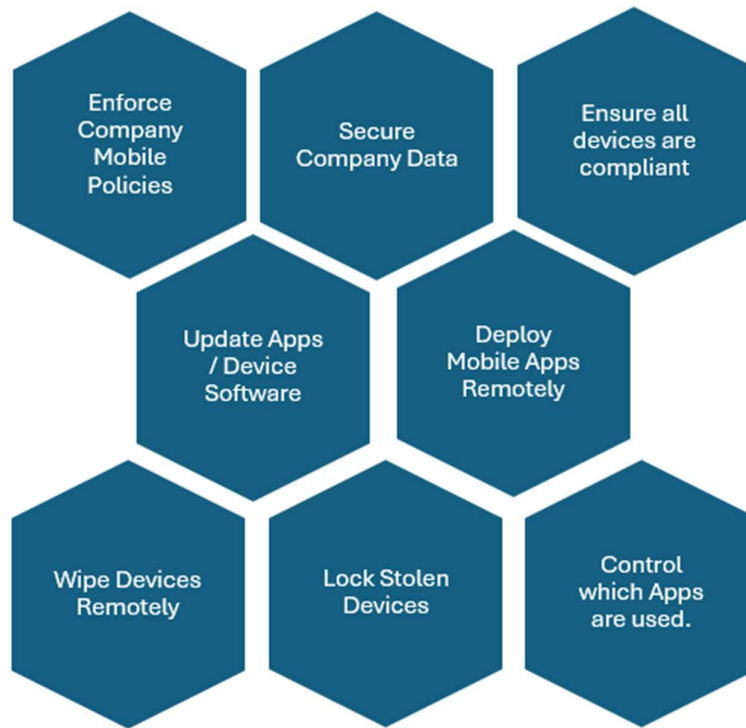
MDM allows **control** and **distribution of security policies** to mobile devices accessing sensitive corporate data in their organizations, ensuring the corporate network is **secure**.

With more and more employees using one or all of these devices, organizations across all shapes and sizes are now turning to mobile device management for **enhanced data and network security** and **improved employee productivity**.

MDM enables configuration of enterprise-grade security policies on mobile devices, making them corporate ready. In the same way that organisations secure data on computers and laptops, the same level of scrutiny and security needs to be applied to mobile devices that are capable of storing and using valuable company data.



Why Mobile Device Management?



- In the same way that organisations secure data on computers and laptops, the same level of scrutiny and security needs to be applied to mobile devices that are capable of storing and using valuable company data.
- MDM for enhanced data and network security and improved employee productivity.
- Sensitive data being held on mobile and within mobile applications the need for mobile security is essential to any business to ensure compliance with GDPR.
- Increased mobile working means that staff are more reliant on mobile devices to work effectively.
- Increased use of mobile applications means that mobiles have become more common for staff.
- The financial impact of mobile misuse is significant to a business.
- The potential impact on a businesses PR if a mobile device provided by the business is misused is high and therefore the need for a strong mobile policy is essential.
- If attempting to be accredited with Cyber Essentials then MDM is essential to being compliant.



Features of Mobile Device Management

There are various MDM solutions available with different features provided as standard. It is essential to understand what the objectives and specific requirements are when deploying a solution to ensure that the aims of the organization are met.

Features include (but not limited to):

Security	Asset Management & Audit	App Management	Policy Enforcement	Feature Restrictions
Work & Personal Device Profiles	View Estate information	App Store Management	Time-fencing	Allow/Disallow use of Camera
Device Encryption	Check Policy Compliance	Deploy approved business apps automatically	Geo-Fencing	Control Screen Lock Timeout
Remote Wipe (Factory Reset)	Audit Trail	Block/Allow list of Apps	SIM Changes	Allow/Disallow use of Browser
Configure Wifi Settings	Control OS Updates and Versions	Auto-App Update Control	WiFi	Allow/Disallow Wi-Fi, Bluetooth, Tethering and GPS
Malware Protection	Configure applications	Control usage of Apps	Enforce pin / fingerprint Authentication	Allow/Disallow voice call, data usage and roaming
Location Tracking	Kiosk Mode		Allow/Disallow use of Screen Capture	

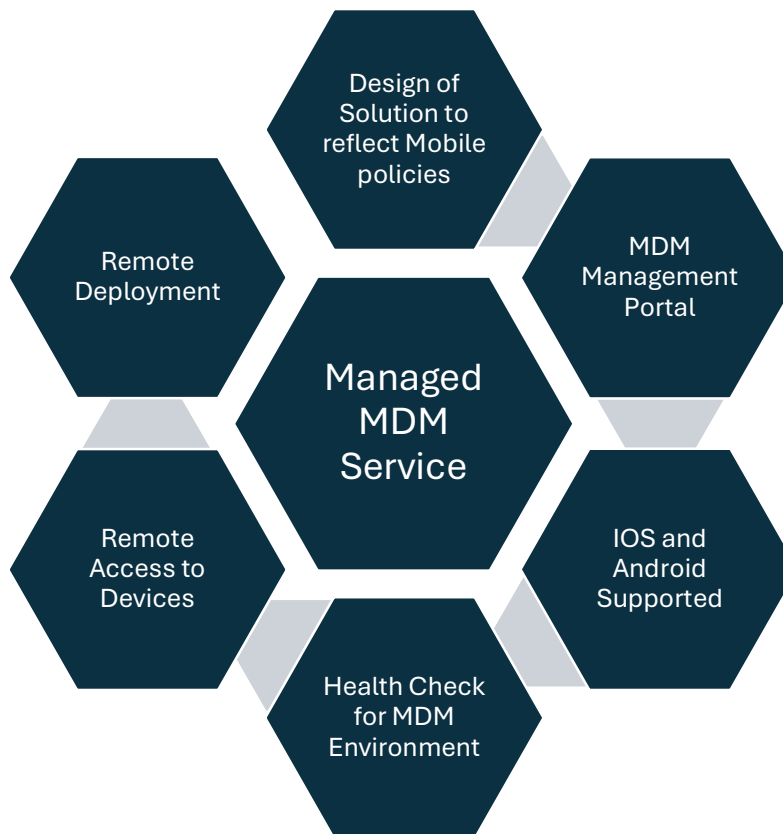


Why SCG for MDM?

SCG are experts in delivering Mobile Solutions and integrate solutions across networks and suppliers. SCG's mobile device Management solution is offered fully managed or license only and can support the design, deployment and ongoing management.

SCG believes that the chosen solution should fit the requirements rather than offering a single solution regardless of the requirements. Therefore, SCG can supply various MDM solutions;

- Samsung Knox Manage (incl. IOS)
- Microsoft Intune
- SOTI
- MaaS360 (License Only)



SCGC can offer a fully managed service including the design and setup of the MDM platform and policies, supported deployment to users and the ongoing management of the solution and support for users.

The fully managed solution offered includes:

- **Scoping** – defining the mobile policies, apps and security to be deployed across devices.
- **Build** – build the environment and profiles that will be deployed out across users
- **Licensing** – purchase of MDM Licenses and assigned to relevant users.
- **Implementation** – Application of relevant user profile to users and setting up of user accounts.
- **Deployment** – deployment across user devices including roll out across new and existing devices.
- **Support** – Support of service during contract including profile changes, deployment of updates and setup of new users and ceasing leavers.



Service Description

Licensing

Provision of user licensing across different MDM solutions in order to deploy and manage MDM across the user estate. Licenses supplied currently:

- Samsung Knox Manage
- SOTI Mobile Control
- Microsoft Intune
- MaaS 360

Setup

Service to include the scoping of requirements and policies to be implemented and the subsequent design and build of the MDM Solution, enrolment processes and user profiles to meet the business requirements.

Implementation

The design and production of working processes to encompass the end-to-end steps to undertake in order to deploy MDM across all users as well as support in setting up the solution to enable the ongoing management and value to be obtained from an effective MDM solution.

Support

Following deployment, the ongoing management and Support is a key consideration in order to derive value from the investment made. SCL provide an ongoing support service to manage the MDM solution from simple backup support for your in-house team to a fully managed support solution that means you do not need to worry.

Support includes but is not limited to setup and management of profiles, factory reset of devices, update of mobile policies, add/remove users.

Remote Deployment of Hardware

Supporting the deployment of handsets from out of the box to MDM deployment, SCL can assist in setting up the deployment portals, enrolling devices into Knox Mobile Enrolment, Apple Business Manager or Google Zero Touch.

