TaaS Service Portfolio
for
Enterprise Mobility
with
Microsoft Intune

MM mobile mentor

mobile mentor

Document Information

Organisation	Mobile Mentor
Project Name:	Telecommunications as a Service
Document Name:	Service Portfolio for Enterprise Mobility with Microsoft Intune
Author/s:	Denis O'Shea
Contributors	Liz Knight, Amanda Gray, Daniel McCarthy, William Todd

Reference documents

Title	Author	Version
Managed Security Service Catalogue	DIA	2019
Service Aggregation Service Catalogue	DIA	2019

1. Service Portfolio for Enterprise Mobility

1.1. Purpose

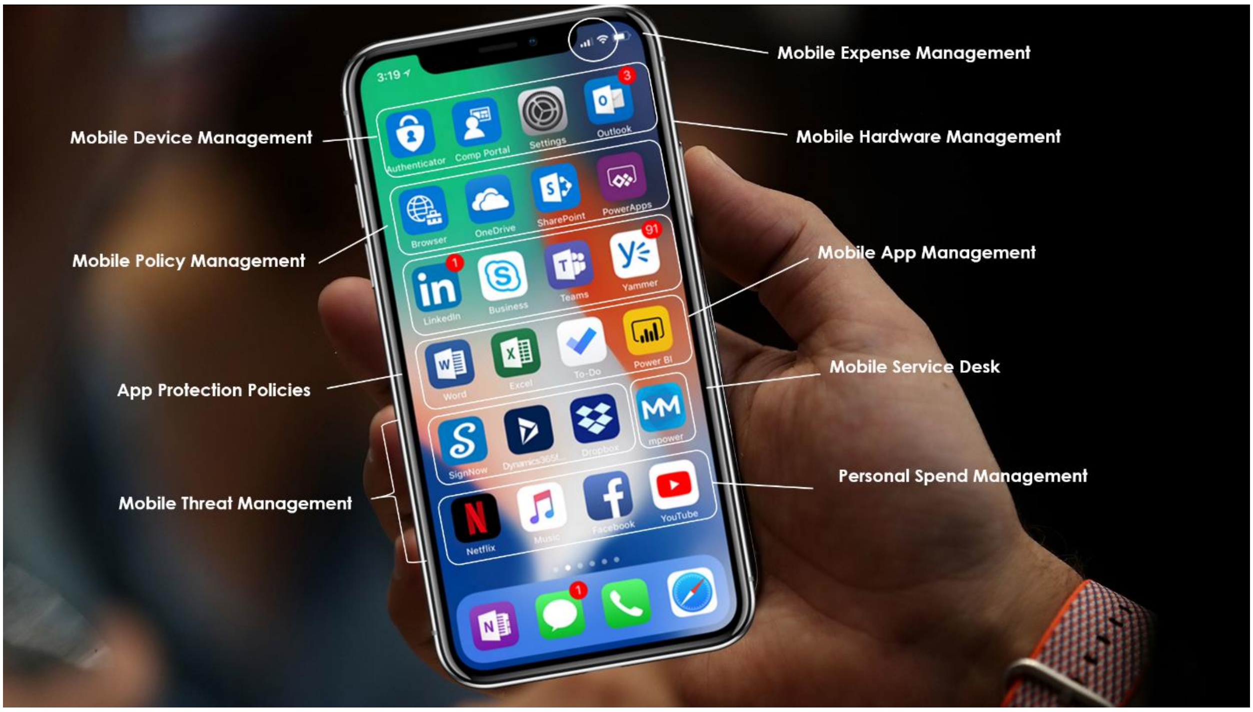
This document outlines the portfolio of services in two service catalogues and provides an explanation of each with the relevant inclusions, exclusions and SLAs.

This is intended to be a buyer's guide to identify the relevant services and product codes.

Prices and detailed service descriptions can be found in the two Service Catalogues on the DIA portal; Managed Security and Service Aggregation.

1.2. Service Map

The illustration below outlines each of the services and how they address enterprise mobility.



Managed Security

1. Intune Management
2. App Protection
3. Policy Management
4. Mobile Threat Management

Service Aggregation

1. Mobile Asset Management
2. Mobile Service Desk
3. Hardware Lifecycle Management
4. Mobile App Management
5. Personal Spend Management

2. Managed Security Catalogue Summary

2.1 Intune Management

Configuration, deployment and management of security policies, profiles, enterprise app store and reporting dashboard for Microsoft Intune.

Microsoft Intune is an alternative mobile device management option that can be used instead of VMware Workspace ONE (AirWatch).

Microsoft Intune requires an EM+S E3 or M365 E3 license and can be configured and managed by Mobile Mentor as below.

Service Element	Service Description
Intune Management	Mobile Mentor provides MDM administration and management services for Intune mobility management via the Microsoft Azure Portal.
Optimised Enrolment	Leverage Apple DEP), Google Zero-Touch, Samsung KME and Android Enterprise to enhance the security, control, administration and user experience for device enrolment.
Enterprise App Store	Standard configuration includes the provision of an enterprise app store to present users with a catalogue of internal apps as well a white-list of approved public apps. Known malicious apps can be black-listed.
App Distribution	Distribute, update and revoke enterprise apps using distribution groups, Google Play for Business, Apple VPP and the enterprise app store.
Live Reporting Dashboard	Dashboard of reports showing the devices under management, time last seen, compliance with policy etc
Reference	*PD1S in the Managed Security Service Catalogue*

2.2 App Protection

Policies to protect data in the Microsoft 365 productivity suite of apps and any app built with the Microsoft Intune app SDK. Works with managed & unmanaged devices, including BYO devices.

Service Element	Service Description
Protect Microsoft 365 Apps	The Mobile App Protection service provides policies to protect corporate data in Office 365 mobile apps such as Outlook, Word and Excel.
Protect Intune SDK Apps	Policies can be configured for any apps built with the Microsoft Intune App SDK.
Unmanaged Devices	App Protection policies can be enabled for apps installed on MDM managed devices (Intune or Workspace ONE) and equally they can be applied to unmanaged devices.
Reference	*PD3S in the Managed Security Service Catalogue*

2.3 Proactive Policy Management

Proactive Policy Management to ensure that the mobile policy is implemented, enforced, monitored and managed.

Service Element	Service Description
Policy Splash Screen	The agency's mobile policy is presented via an interactive mobile app with a readable, bullet point summary and questions related to data security and privacy.
Policy Sign-on-Screen	The employee accepts the terms, signs on-screen and submits the signed policy which is saved to a database accessible by the Agency's HR department.
Policy Management	If a policy breach or security incident occurs, the organisation is equipped with a signed policy from the user and is able to take the appropriate action.
Compliance Monitoring	Mobile Mentor monitors the devices under management for compliance with policy and identifies non-compliance events to be addressed.
Compliance Monitoring	We report on policy compliance through the ZOOOOM dashboard. Every three months we review the policy and make adjustments to reflect industry threats, organisational changes and the most common breaches.
Reference	*PD4S in the Managed Security Service Catalogue*

2.4 Mobile Threat Management (TaaS Certified)

App and network scanning and analysis to detect, assess, report and mitigate the risks of malware and malicious apps and networks.

Service Element	Service Description
App Reputation Scanning	App reputation scanning using an industry leading platform to detect malicious apps and determine risk severity. Detection of malicious network activity on devices using Wi-Fi.
Threat Analysis	Industry scanning and threat analysis to assess the security posture of the device OS, EMM platform, AV and apps under management;
Severity Scoring	New threats or changes graded by severity and likelihood by a qualified security analyst and documented for auditability;
Risk Mitigation	Software patching, app updates, policy changes and changes to system settings to mitigate identified risks.
Risk Reporting	Reporting on device security posture, risk scores and system health.
Reference	*PD5S in the Managed Security Service Catalogue*

3. Service Aggregation Catalogue

3.1 Mobile Asset Management

Mobile Asset Management is the combination of 3 services:

1. Mobile expense management (analysis and optimisation);
2. Rapid replacement, service restoration, repair management for devices;
3. Reporting Dashboard

Service Element	Service Description
Data Warehouse	Extraction of mobile usage and spend to an independent warehouse to match the Agency's cost centers and organisation structure.
Analysis & Optimisation	In-depth analysis of monthly spend to identify outliers, trends and savings opportunities.
Implement Changes	Implement the agreed changes directly in the billing systems of the mobile service providers to benefit the Agency.
Avoid cost blow-outs	Real-time expense management process to provide early identification of overage and rogue usage to mitigate cost blow-outs.
Rapid Replacement	Provision of a loan device for up to 10 days for corporate and BYO devices.
Service Restoration	Service restoration to help the impacted user to restore their settings, apps, services and data on a new device.
Repair Management	Device triage, warranty management and repair process management.
Reporting Dashboard	Real-time dashboards for a) policy compliance, b) device security, c) service desk performance, d) usage & spend reports and e) user satisfaction.

Reference	*PD1A in the Aggregation Service Catalogue*

3.9 Service Desk

24 x 7 specialist team for mobile procurement, provisioning, enrolment and user support through the **m.power** mobile support app.

This service applies to all mobile devices, all networks, with all major MDM providers, and all ownership models (BYOD, CYOD & COPE).

Service Element	Service Description
24 x 7 x 365 Mobile Service Desk	Mobile experts with the appropriate skills and experience, based in Auckland and Wellington, or at the customer's premises by arrangement.
Procurement	Integration with the Agency's approval process and delivery of requested services within 5 business days.
Assisted Enrolment	Visual and intuitive enrolment guides with phone support to assist users with the process of enrolling their devices.
Support Portal and Knowledge Base	Service portal with knowledge base articles specific to the Agency's mobile policy, devices, apps and processes.
User Support App	Support app for the end user to engage with Mobile Mentor from their mobile device.
Reference	*PD2A in the Aggregation Service Catalogue*

3.10 Personal Spend Management

Separate business and personal usage for end users and cost center managers and reconcile employee reimbursements for personal usage.

Unique process for identification, reimbursement and reconciliation of personal usage for end-users and cost center managers.

Service Element	Service Description
Itemised Reports Per User	Detailed monthly reports separating personal and business usage for each individual user, each cost center manager and each general manager.
Reimbursement via Payroll	Automated reimbursement process integrated to the Agency's payroll process.
Reconciliation with Cost Centers	Reconciliation of employee reimbursements with the cost centers to provide complete transparency and accountability.
Reference	*PD3A in the Aggregation Service Catalogue*

3.11 Hardware Lifecycle Management

Management of the hardware life-cycle from device selection, accessories, repair and secure erasure at end of life.

Hardware lifecycle management service that applies to all mobile devices and all ownership models (BYOD, CYOD & COPE).

Service Element	Service Description
Device Shortlist	Mobile Mentor publishes a "sensible short-list" of devices that can be secured, managed and supported by their MDM platform.
Case or Screen Protector	All smartphones and tablets receive a silicone case or a screen protector to extend the life of the device.
Device Refresh	Device upgrades managed according to any available carrier hardware subsidies or internal refresh program.
Asset Tagging	Maintain a configuration management database of all hardware assets under management.
Secure Erasure	Devices are wiped beyond the level of a factory reset to ensure that they can be re-used without any risk of residual data remaining on the device.
Reference	*PD4 in the Aggregation Service Catalogue*

3.12 App Management

App distribution through the enterprise app store, release management, Level 1 support and analytics for enterprise apps.

Management of the portfolio of productivity apps (both public and enterprise apps) deployed to Agency devices.

Service Element	Service Description
Enterprise App Store	Management of the Agency's app store with 10 standard public apps per OS.
Apple VPP Management	Administration of the Apple VPP account and management of app licenses to the appropriate distribution groups.
Level 1 App Support	Support internal users with app installation and connectivity for up to 5 vertical / Line Of Business apps.
Release Management	Planning, approval, basic testing, rollout, communications & documentation for a combined total of 30 app updates p.a. for internal users.
App Analytics	Analysis and reporting of app inventory, trends, usage (if available) and opportunities for productivity improvement.
Reference	*PD6 in the Aggregation Service Catalogue*

3.13 Fleet Management

Combination of Service Desk, Asset Management, Hardware Lifecycle Management, Expense Management and Personal Spend Management with all reporting services.

a) Mobile Expense Management
b) Rapid Recovery
c) Level 1 Service Desk
d) Personal Spend Management
e) Hardware Life-Cycle Management
f) Fleet Management App