Intune Packaged Service Offering

Prepared by impeltec Pty Ltd

www.impeltec.com

+61 3 9018 7460

L31, 120 Collins Street
Melbourne VIC 3000

Table of Contents

1 Overview

The Intune Packaged Service Offering provides a professional, fast, and efficient configuration for Autopilot that will have new devices up and running, configured and managed in line with Microsoft's modern management approach.

Microsoft Intune is a cloud-based service that focuses on mobile device management (MDM) and mobile application management (MAM). Windows Autopilot simplifies provisioning and enrolling devices. With Microsoft Intune and Autopilot, you can give new devices to end-users without the need to build, maintain, and apply custom operating system images.

This document details the Intune Packaged Service Offering that can be selected for each of the two (2) packages:

- Windows Device Management
- Mobile Device Management (MDM)

and three (3) tiers:

- Standard
- Advanced
- Premium

1.1 Our Philosophy

impeltec provides its customers with consistent and reliable IT services by delivering a model that focuses on repeatability, standardisation and automation. Our specialist end-user skills ensure that not only are the technologies and services running smoothly but also that the customer is satisfied with the IT services being provided.

impeltec strongly believes in building honest, friendly and ongoing partnerships with its customers. We seek to gain an understanding of our customers' business and IT philosophy. In doing so, we aim to deliver the highest quality and most cost-effective and efficient solutions that ensure we meet our customers' needs. We work closely with our customers, maintaining constant contact through an open-door policy, ensuring an outcome where all parties can grow from the experience.

1.2 Experience

impeltec specialises in end-user workplace services and cloud technologies. We have vast experience with designing and building SOE solutions for Windows with a high focus on automation, application packaging, desktop deployment projects, and Microsoft infrastructure and cloud technologies. We have strong IT skills in a number of systems management platforms including Microsoft Endpoint Configuration Manager and Microsoft Intune. As a Gold Microsoft Partner with the Cloud Platform and Cloud Productivity competencies, impeltec focuses on Microsoft cloud technologies including Azure, Microsoft 365 and Intune.

We have a strong track record of helping our customers develop their end-user computing IT strategy and direction and can assist with planning activities for major transformation projects. impeltec has partnered with many customers on their journey into the Microsoft cloud.

2 Service Offerings

The service offerings have been designed to provide an initial Intune environment to get you up and running; it is not designed as an all-encompassing configuration. The expectation is that it may be further enhanced after this initial engagement, which can be delivered as additional scope if required.

There are two (2) packages that can be selected either independently or together as a comprehensive package, these are:

- Windows Device Management
- Mobile Device Management (MDM)

Each of these packages includes a set of base inclusions to ensure Intune is fully operational for each package, these are outlined in section *2.1 Inclusions*

Within each package there are three (3) tiers that can be selected:

- Standard
- Advanced
- Premium

This section details the inclusions for each of the two packages and three tiers.

2.1 Inclusions

The following table provides a comparison for the inclusions for each package and tier. Definitions for configuration items can be found in *Section 3 Packages.*

2.1.1 Base inclusions

Each package delivers the base inclusions dependant on the tier as defined in the table below:

Tiers:	Standard	Advanced	Premium
Consultation (Hours)	1	2	4
Tenant configuration	Yes	Yes	Yes
Company branding	Yes	Yes	Yes
Store apps - Microsoft 365	Yes	Yes	Yes
As-Built Design document	Yes	Yes	Yes
Pilot Testing (No. of Devices)	3	3	5
Support/Knowledge sharing (Hours)	2	4	8

2.1.2 Windows Device Management Package

The Window Device Management package delivers the inclusions defined in the table below based on tier selected:

Tiers:	Standard	Advanced	Premium
Auto-enrollment configuration	Yes	Yes	Yes
Device/User groups	1	3	5
Configuration profiles	1	3	5
Device compliance policies	0	1	3
Update policies	1	2	3
Endpoint security policies	0	1	3
Analytics and reporting	No	Yes	Yes
WiFi/VPN configuration	0	1	1
Conditional Access policies	0	1	3
Store configuration	Microsoft	Microsoft	Microsoft
Store apps – Other	1	3	5
Windows Autopilot (Add-on)			
Windows Autopilot provisioning	Add-on		
- Pre-provisioned deployment	Option (Windows Autopilot provisioning add-on must be selected)		
- Hybrid Azure AD join	Option (Windows Autopilot provisioning add-on must be selected)		

2.1.3 MDM for non-Windows Devices Package

The MDM for non-Windows devices package delivers the inclusions defined in the table below based on the tier selected:

Tiers:	Standard	Advanced	Premium
Enrollment configuration	1	2	4
MAM App Protection Policies	0	1	2
Device/User groups	1	2	4
Configuration profiles	1	2	4
Compliance policies	1	2	4
Update policies	No	iOS, iPadOS	iOS, iPadOS
Conditional Access policies	0	1	3
Store configuration	Microsoft	Microsoft, Apple, Google	Microsoft, Apple, Google
Store apps - Other	1	3	5

3 PACKAGES

The following subsections detail the configuration items in scope for each package. The extent to which these are configured or implemented is dependent on the package and service tier selected as defined in *Section 2* Service Offerings.

3.1 BASE INCLUSIONS

Base inclusions are part of the scope regardless of the package and tier selected; these are included as part of all engagements, where required.

3.1.1 Consultation

All packages include a defined amount of consulting hours with the <Customer>'s IT coordinator to understand the key Intune operational and business requirements.

3.1.2 Tenant configuration

For all packages, an Intune tenant in the Microsoft cloud is required. Each package provides assistance with the following activities:

- Ensure an Intune tenant is activated and associated with the correct Microsoft cloud services tenancy for <Customer>
- Add and validate up to three (3) custom domain name(s)
- Ensure Intune is the MDM authority

3.1.3 Company branding

The Intune Company Portal is used to enroll devices and install apps, it will be visible on users' devices. Each tier includes look and feel customisation to match 's organisational themes, including:

- Logo
- Colour
- Background

3.1.4 Store apps - Microsoft 365

Intune can remotely deploy apps to users' devices. Although each packaged service has various inclusions for apps. The base service includes the configuration of *Microsoft 365 Apps for Windows 10 and later*. This includes:

- Deployment configuration of Microsoft 365 Apps
- Advice on architecture and update channel selection
- Enabling or disabling standard Office apps:
  - Access
  - Excel
  - OneNote
  - Outlook
  - PowerPoint
  - Publisher
  - Skype for Business
  - Teams
  - Word
- Additional licensed Office apps:
  - Project
  - Visio

Microsoft Office 365 ProPlus has been renamed to *Microsoft 365 Apps for Enterprise,* commonly referred to as *Microsoft 365 Apps*.

3.1.5 Pilot Testing

The Intune configuration and functionality will be tested on a defined number of test devices. This applies to both Windows and MDM devices depending on the package selected.

3.1.6 As-Built Design Document

For all packages an As-Built Design document will be supplied.

3.1.7 Support/Knowledge sharing

After delivering the selected package, a defined number of hours for supporting IT staff is included dependent on the tier selected. This includes general technical support, knowledge sharing and Q&A, and assistance with using Intune or any other services delivered. Support hours are to be consumed either during the project or with 2 months of handover.

3.2 Windows Device Management

Windows devices can be managed using Intune, including but not limited to configuration of user and device policies, software and servicing updates, security, and app deployment. If this package is selected, Intune will be configured for the management of Windows 10 and later devices. The following subsections detail each component as defined in the inclusions for each packaged service offering.

3.2.1 Auto-enrollment

Auto-enrollment can be configured to automatically enroll Windows 10 and later devices with Intune. The service includes the configuration of auto-enrollment.

3.2.2 Device/User groups

Configuration is included for a defined number of Azure AD user or device groups to be used for Windows device management. These may be used for license assignment, logical groupings, or app and configuration assignments.

3.2.3 Device compliance policies

Compliance policies can help protect organizational data by requiring users and devices to meet requirements and include:

- Defining the rules and settings that users and devices must meet to be compliant
- Actions that apply to devices that are noncompliant

Consultation is included to determine the rules, settings and actions that are required for <Customer>. The service includes the configuration of a defined number of device compliance policies for Windows devices. Each device compliance policy is limited to a maximum of 10 individual settings.

Below is a top-level table of some of the possible Windows 10 compliance policy settings:

Intune Windows Compliance policy Settings (top level)		
Configuration Manager Compliance System Security	Device Health Microsoft Defender for Endpoint	Device Properties

3.2.4 Update policies

Intune manages the install of Windows 10/11 software updates from Windows Update for Business, including:

- Update rings for Windows 10 and later
- Feature updates for Windows 10 and later

Consultation is included to determine the updates and schedules that are required for <Customer>. The service includes the configuration of a defined number of update policies for Windows devices.

3.2.5 Configuration profiles

Device profiles allow for adding and configuring settings, and pushing these settings to devices in your organization. Configuration is included for a defined number of configuration profiles for Windows device management. This includes the following configuration profile types:

- Administrative templates (Windows)
- Device restrictions

Consultation is included to determine what settings are required for <Customer>. Each configuration profile is limited to a maximum of 30 individual settings.

Below is a top-level table of some of the possible configuration settings:

Intune Windows Configuration Profile Settings (top level)			
Above Lock	Accounts	Administrative Templates	Application Defaults
Auditing	Authentication	BitLocker	BITS
Bluetooth	Browser	Camera	Cellular
Connectivity	Control Policy Conflict	Converters	Credential Providers
Cryptography	Data Protection	Defender	Deliver Optimization
Device Guard	Device Health Monitoring	Device Lock	Display
DMA Guard	Education	Enterprise Cloud Print	Experience
Exploit Guard	Firewall	Games	Handwriting
Kerberos	Kiosk Browser	Lanman Workstation	Licensing
Loader Override Settings	Local Policies Security Options	Lock Down	Maps
Memory Dump	Microsoft Office 2016	Microsoft App Store	Microsoft Defender for Endpoint
Microsoft Edge	Network Isolation	New and Interests	Notifications
OneDrive	Power	Privacy	Reboot
Remote Desktop	Search	Security	Settings
Shared PC	Smart Screen	Speech	Start
Storage	System	System Services	Task Manager
Task Scheduler	Text input	Time Language Settings	Troubleshooting
User Rights	Widgets	Windows Defender Security Centre	Windows Hello for Business
Windows Ink Workplace	Windows Logon	Windows Update for Business	Wireless Display

3.2.6 Endpoint security policies

Intune endpoint security policies to manage security settings on devices. Each endpoint security policy supports one or more profiles. These profiles are similar in concept to a device configuration policy template, a logical group of related settings. The following policy types are included in this service:

- Antivirus
- Disk encryption
- Account protection

Consultation is included to determine what security settings are required for <Customer>. The service includes the configuration of a defined number of endpoint security policies for Windows devices. Each endpoint security policy is limited to a maximum of 15 individual settings

3.2.7 Analytics and reporting

Microsoft Intune reports allows you to more effectively and proactively monitor the health and activity of endpoints across your organization, and also provides other reporting data across Intune. For example, you will be able to see reports about device compliance, device health, and device trends.

Microsoft can collect event data and provide recommendations to improve performance on your Windows devices. Endpoint Analytics analyses this data, and can recommend software, help improve start-up performance, and fix common support issues.

A demonstration of how to use reports to monitor environment is included, as well as the enablement of data collection for Windows Health Monitoring and Endpoint Analytics.

3.2.8 WiFi/VPN configuration

Intune can deploy your Wi-Fi settings and virtual private network (VPN) connection settings to users and devices.

Consultation is included to determine what WiFi or VPN settings are required for <Customer>. The service includes the configuration a defined number of WiFi or VPN policies for Windows devices.

3.2.9 Conditional Access policies

Conditional Access controls the devices and apps that can connect to your email and company resources. Conditional Access is an Azure Active Directory capability that is included with an Azure Active Directory Premium license.

Consultation is included to determine what controls are required for <Customer>. The service includes configuration for a defined number of conditional access policies for Windows devices.

3.2.10 Store configuration

Microsoft Store apps can be added into Intune for deployment to users and devices.

3.2.11 Company Portal App

The Company Portal app installation is included within the base service. When the Company Portal app is installed, users open it, and see the apps your organization makes available. Users select an app, and install it.

3.2.12 Store apps – Other

Consultation is provided to determine which apps from the Microsoft Store are required for <Customer>. The service includes the configuration of a defined number of Microsoft Store apps for deployment to Windows users or devices.

3.3 Windows Autopilot Add-on

These additional Windows Autopilot services can be individually selected in addition to the Windows Device Management package.

3.3.1 Windows Autopilot provisioning

Windows Autopilot helps organizations easily provision new devices by using the preinstalled OEM image and drivers. This lets end users to get their devices business-ready by using a simple process.

If the Windows Autopilot Provisioning add-on is selected, configuration of one (1) Autopilot deployment profile to enable Windows Autopilot provisioning is included, as well as testing to ensure functionality and validation of the applied Intune configuration. Activities included within the Windows Autopilot provisioning add-on include:

- Infrastructure requirements
- Configuration of device enrollment
  - Enrollment restrictions
- Enrollment Status Page (ESP) configuration
- Testing of the Windows Autopilot provisioning process on one (1) device
- Testing on a single version of Windows (eg Windows 11 only)
- Autopilot deployment process documentation

Only one type of application can be assigned to Autopilot deployments, i.e you cannot mix Store apps with Win32 Line of Business apps.

3.3.1.1 Option: Pre-provisioned devices

Windows Autopilot can also provide a pre-provisioning service that helps partners or IT staff pre-provision a fully configured and business-ready Windows PC. From the end user's perspective, the Windows Autopilot user-driven experience is unchanged, but getting their device to a fully provisioned state is faster as more of the device configuration is performed before device delivery to the user.

Configuration of one (1) Autopilot deployment profile to enable Windows Autopilot for pre-provisioned devices is included, as well as testing of the technician and user flows, and validation of the functionality.

The Windows Autopilot white glove feature has been renamed to Windows Autopilot for pre-provisioned deployment.

This option is an extension to the *Windows Autopilot provisioning* service.

3.3.1.2 Option: Hybrid Azure AD join

By default, Windows Autopilot will join devices to Azure AD. However, <Customer> may have an on-premises Active Directory Domain Services (AD DS) environment and wish to configure hybrid Azure AD join (where devices are both joined to on-premises AD and registered with Azure AD).

The service includes the installation and configuration of the Intune Connector for Active Directory within the <Customer> on-premises environment. This includes the configuration of one (1) Autopilot deployment profile and testing of hybrid Azure AD join functionality as part of the Windows Autopilot provisioning service.

This option is an extension to the *Windows Autopilot provisioning* service (and may be used in conjunction with the *Pre-provisioned devices* option).

3.4 Mobile Device Management (MDM) - Non-Windows

This service focuses on the configuration of Intune for management of non-Windows devices, which may include iOS/iPadOS, macOS, or Android devices.

3.4.1 Enrollment configuration

Intune allows for the management of <Customer>'s devices and apps, and controls how users access company data. To use this mobile device management (MDM), the devices must first be enrolled in the Intune service. When a device is enrolled, it's issued an MDM certificate. This certificate is used to communicate with the Intune service.

Configuration of Intune for enrollment of a defined number of platforms, including iOS/iPadOS, macOS, and/or Android devices, is included.

3.4.2 MAM - App protection policies

Mobile Application Management (MAM) app protection policies allows for the management and protection of organizational data within an application. These rules ensure an organization's data remains safe or contained in a managed app. A policy can be a rule that is enforced when the user attempts to access or move corporate data, or a set of actions that are prohibited or monitored when the user is inside the app.

Configuration of a defined number of MAM App Protection Policies is included.

3.4.3 Device/User groups

Configuration of a defined number of Azure AD user or device groups to be used for MDM is included. These may be used for license assignment, logical groupings, or app and configuration assignments.

3.4.4 Configuration profiles

Device profiles allow for adding and configuring settings, and pushing these settings to devices. Configuration of a defined number of configuration profiles for MDM devices is included for the following configuration profile types:

- Device features (macOS, iOS, iPadOS)
- Device restrictions
- Email

Consultation to determine which settings are required for <Customer> is included. Each configuration profile is limited to a maximum of 30 individual settings.

3.4.5 Device compliance policies

Compliance policies can help protect organizational data by requiring users and devices to meet some requirement, which includes:

- Definition of the rules and settings that users and devices must meet to be compliant
- Actions that apply to devices that are non-compliant

Consultation to determine which rules, settings and actions are required for <Customer> is included, as well as configuration of a defined number of device compliance policies for MDM devices. Each device compliance policy is limited to a maximum of 10 individual settings.

3.4.6 Update policies

Intune manages the install of software updates for supervised iOS/iPadOS devices. Supervised devices are devices that enrolled using either Apple Business Manager or Apple School Manager.

Consultation to determine which updates and schedules are required for <Customer> is included, as well as configuration of a defined number of update policies for MDM devices.

3.4.7 Conditional Access policies

Conditional Access controls the devices and apps that can connect to your email and company resources. Conditional Access is an Azure Active Directory capability that is included with an Azure Active Directory Premium license.

Consultation to determine what controls are required for <Customer> is included, as well as configuration of a defined number of conditional access policies for MDM devices.

3.4.8 Store configuration

Microsoft Store, Google Play and iOS store apps can be added into Intune for deployment to users and devices. Integration of the required stores with Intune is included.

3.4.9 Store apps – Other

Consultation to determine what apps from the Microsoft Store, iOS store or Google Play are required for <Customer> is include, as well as configuration of a defined number of apps for deployment to MDM users or devices.