



# Microsoft Security Labs

**Microsoft Modern Work Team**

Dicker Data

March 2024



# Notable information

Demo labs via your MPN ([cdx.transform.microsoft.com](https://cdx.transform.microsoft.com))

Contact: [microsoft.presales@dickerdata.com.au](mailto:microsoft.presales@dickerdata.com.au)

We are recording the session – We will share a link to the recording AFTER the event – you cannot download it directly from Teams.

# Series Agenda

## **Part 1 (Tuesday, 27<sup>th</sup> February)**

- Security Foundations
- Identity Security
- Email Protection
- Defender for Business

## **Part 2 (Today, 5<sup>th</sup> March)**

- Autopilot
- Intune & Security
- Endpoint Management

## **Part 3 (Tuesday, 12<sup>th</sup> March)**

- Information Governance
- Purview
- Introduction to Copilot for Microsoft 365
- Copilot Readiness



DICKER  
DATA

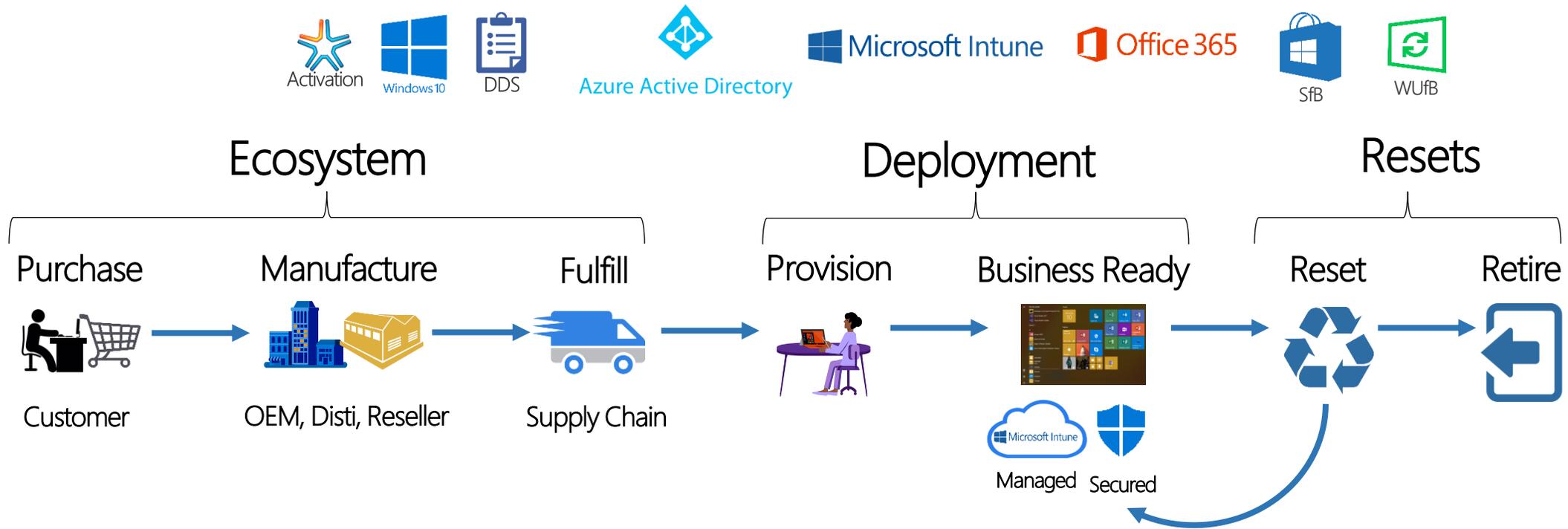


# Autopilot, Intune & Security



# Entra ID Join

- Entra ID Registered vs Joined
- MDM Only
- Hybrid Join – Should you use it?
- Brief Demonstration



Autopilot delivers zero touch **deployment & reset** experiences powered by Microsoft 365

# Why Autopilot?

- Reduce the time IT spends on deploying, managing & retiring devices
- 4-hours saved per device
- 67% reduction in support calls
- 62% of IT admins - less effort managing Surface devices
- Reduce the infrastructure required to maintain the devices
- Maximize ease of use for all types of end user
- Empower resources to innovate and add value



# What is Autopilot pre-provisioned deployment

ASCEND

- Device is intercepted by distribution or partner
- Unboxed and OOBE is executed
- Configuration deployed
- Includes all apps, security, patching
- Re-boxed, shipped to user – can include asset tagging, keyboard, mouse etc.
- Ready to use, fully provisioned!





## Why Dicker Data?

- Free 24 x 7 x 365 support
- We do the heavy lifting including White Glove/pre-provisioned deployment
- Standard, Advanced and Custom Autopilot services
- Seamless Autopilot integration using the Dicker Data portal
- Device as a Service for full lifecycle management



# Summary

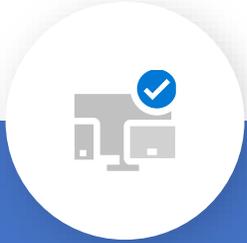
ASCEND

1. Intune is cloud Mobile Device Management (MDM & MAM)
2. To use Intune, devices need to be enrolled
3. Devices can be enrolled via GPO, a script, Azure AD or by adding a work or school account to the device settings
4. Autopilot is automated provisioning of the OS, apps and configuration
5. Autopilot also enrolls a device in Intune via Azure AD Join and it uses Intune for apps and configuration deployment

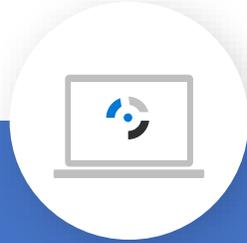
# Autopilot Administrative Experience



# Intune Enrollment Methods



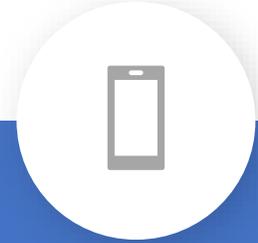
Bulk Enrollment



Windows Enrollment



Apple Enrollment



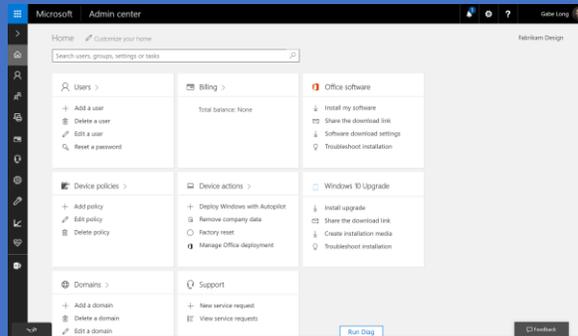
Android Enrollment



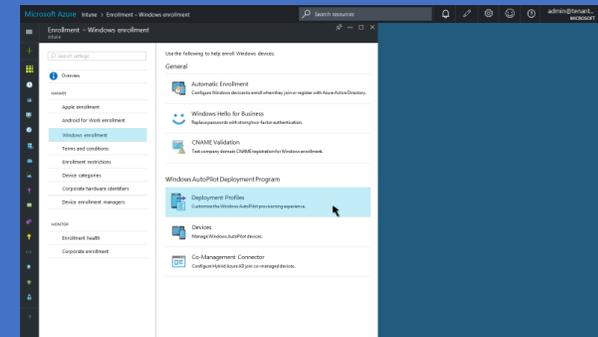
# Bulk Enrollment



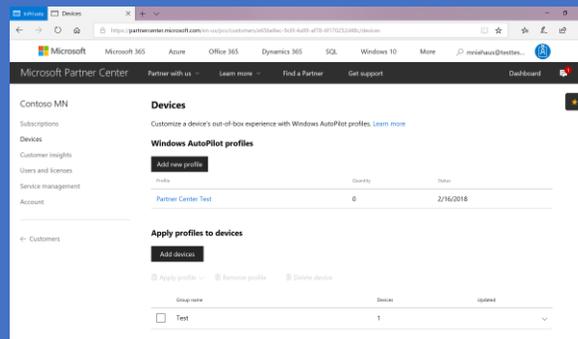
## Admin Center



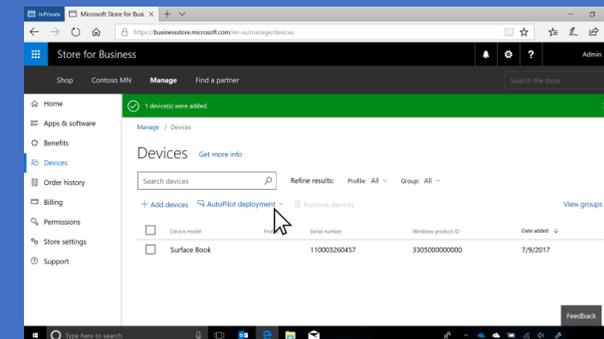
## Microsoft Intune



## Partner Center



## Microsoft Store for Business





# Bulk Enrollment CSV and Barcode



Device Serial Number	Windows Product ID	Hardware Hash
1478271758	3.40629E+12	ADiUQbLG97Sqq6po1t3LIT/ivdsH6ICv+NfteXYQ06PfM6/uZPKCd5gCPQOLYJMZ1c48FRucT+nYKZeUnoqelvNyDqSbRBdx
1478271759	3.40629E+12	BDiUQbLG97Sqq6po1t3LIT/ivdsH6ICv+NfteXYQ06PfM6/uZPKCd5gCPQOLYJMZ1c48FRucT+nYKZeUnoqelvNyDqSbRBdx
1478271760	3.40629E+12	CDiUQbLG97Sqq6po1t3LIT/ivdsH6ICv+NfteXYQ06PfM6/uZPKCd5gCPQOLYJMZ1c48FRucT+nYKZeUnoqelvNyDqSbRBdx





# Enroll Devices



The screenshot displays the Microsoft Endpoint Manager admin center interface. The breadcrumb navigation shows 'All services > Devices > Windows'. The main heading is 'Windows | Windows enrollment'. Below this, there is a search bar and a 'Learn more' link. The left-hand navigation pane includes 'Windows devices', 'Windows enrollment', and 'Windows policies'. The 'Windows enrollment' section is expanded, showing several configuration options: 'Automatic Enrollment', 'Windows Hello for Business', 'CNAME Validation', 'Enrollment Status Page', 'Deployment Profiles', 'Devices', and 'Intune Connector for Active Directory'. Each option includes a brief description of its function.

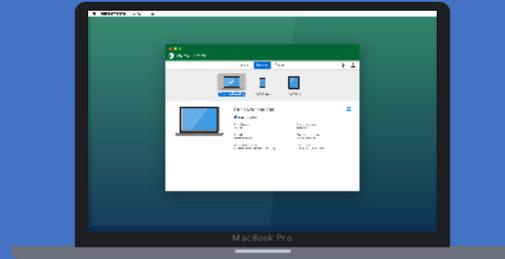
- Bulk Enrolment CSV file format
- PO number or unique name
- Related Device Group
- Admin Center is the recommended method
- Registration Permissions
- Dicker Data Portal



# Mobile Device Provisioning



Apple iOS



MacOS



MacOS  
(with Jamf)



Android

- Device Enrollment Program
- Apple School Manager
- Apple Business Manager
- Supervised Mode
- Intune APP managed

- Deploying cert and settings
- Zero-touch (DEP)
- Conditional access
- Device wipe, encryption

- Intune MDM features +
- Extensive inventory
- Scripting support
- Depth of security controls
- Self-service controls

- Android Enterprise (ZTE)
- Samsung Knox (KME)
- Kiosk mode
- Work Profiles
- Intune APP managed



# 5 Simple Steps

ASCEND

The screenshot displays the Microsoft Endpoint Manager admin center interface. The breadcrumb navigation shows 'All services > Devices > Windows'. The main heading is 'Windows | Windows enrollment'. A search bar is present with the text 'Search (Cmd+I)'. Below the search bar, there is a link to 'Learn about the seven different ways a Windows 10 PC can be enrolled into Intune by users or admins. Learn more'. The left-hand navigation pane includes 'Windows devices', 'Windows enrollment', and 'Windows policies'. The 'Windows enrollment' section is expanded, showing 'Automatic Enrollment', 'Windows Hello for Business', 'CNAME Validation', 'Enrollment Status Page', 'Deployment Profiles', 'Devices', and 'Intune Connector for Active Directory'. The 'Automatic Enrollment' card describes configuring Windows devices to enroll when they join or register with Azure Active Directory. The 'Windows Hello for Business' card describes replacing passwords with strong two-factor authentication. The 'CNAME Validation' card describes testing company domain CNAME registration for Windows enrollment. The 'Enrollment Status Page' card describes showing app and profile installation statuses to users during device setup. The 'Deployment Profiles' card describes customizing the Windows Autopilot provisioning experience. The 'Devices' card describes managing Windows Autopilot devices. The 'Intune Connector for Active Directory' card describes configuring hybrid Azure AD joined devices.

1. Enable enrollment
2. Check DNS
3. Create a profile
4. Assign to Entra ID Device Group
5. Enrollment Status Page



# Step 1 – Enable Automatic Enrollment



Microsoft Endpoint Manager admin center

Home > Devices > Enroll devices >

## Configure

Microsoft Intune

Save Discard Delete

MDM user scope  None  Some  All

MDM terms of use URL  ✓

MDM discovery URL  ✓

MDM compliance URL  ✓

[Restore default MDM URLs](#)

MAM user scope  None  Some  All

MAM terms of use URL  ✓

MAM discovery URL  ✓

MAM compliance URL  ✓

[Restore default MAM URLs](#)

- MDM User Scope
- MAM vs MDM precedence for BYoD
- MDM for Corporate
  - Autopilot
  - Group Policy
  - User is a Device Enrolment Manager
  - Bulk Enrolment



## Step 2 – Check DNS



### CNAME Validation ×

Windows enrollment

Configuring a CNAME in your DNS saves your users from having to enter the address of the MDM server when enrolling their Windows devices. [Learn more](#)

After configuring the CNAME resource records in your DNS, enter the corresponding domain here to confirm that it has been configured correctly. Changes to DNS records might take up to 72 hours to propagate.

Domain

Test

✓ CNAME for intune.mobi is configured correctly.

- DNS records are optional records during custom domain setup
- Can be configured at any time
- Refer to the domain registrar or DNS authority

enterpriseenrollment	CNAME	1h	enterpriseenrollment.manage.microsoft.com.
enterpriseregistration	CNAME	1h	enterpriseregistration.windows.net.



## Step 3 – Enable Enrollment Profile

ASCEND

Microsoft Endpoint Manager admin center

Home > Devices > Enroll devices > Windows Autopilot deployment profiles > AutopilotAAD

### AutopilotAAD | Properties

Windows PC

Search (Cmd+/)

Overview

Manage

- Properties
- Assigned devices

**Basics** Edit

Name	AutopilotAAD
Description	--
Convert all targeted devices to Autopilot	Yes
Device type	Windows PC

**Out-of-box experience (OOBE)** Edit

Deployment mode	User-Driven
Join to Azure AD as	Azure AD joined
Language (Region)	English (Australia)
Automatically configure keyboard	No
Microsoft Software License Terms	Hide
Privacy settings	Hide
Hide change account options	Hide
User account type	Administrator
Allow White Glove OOBE	Yes
Apply device name template	Yes
Enter a name	LAB%RAND:3%

- User vs Self-deploying
- Convert all target devices to Autopilot
- Hybrid vs EID Joined
- User type
- Allow Autopilot
- Naming template
- Device Group Assignment



# Step 4 – Create Device Group



Microsoft Endpoint Manager admin center

Dashboard > Groups >

## New Group

Group type \* ⓘ  
Security

Group name \* ⓘ  
CustomerA

Group description ⓘ  
Purchase Order 12345678

Azure AD roles can be assigned to the group (Preview) ⓘ  
Yes No

Membership type \* ⓘ  
Dynamic Device

Owners  
No owners selected

Dynamic device members \* ⓘ  
[Edit dynamic query](#)

Create

Configure Rules Validate Rules (Preview)

You can use the rule builder or rule syntax text box to create or edit a dynamic membership rule. ⓘ [Learn more](#)

And/Or	Property	Operator	Value
	devicePhysicalIds	Any	( -eq "

+ Add expression

**Rule syntax** [Edit](#)

```
(device.devicePhysicalIds -any ( -eq "[PurchaseOrderId]:12345678"))
```



# Step 5 – Enrolment Status Page



The screenshot shows the Microsoft Endpoint Manager admin center interface. The left-hand navigation pane includes sections for Home, Dashboard, All services, FAVORITES, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area displays the 'HomeLab Enrollment Status Page | Properties' configuration page. At the top, there is a breadcrumb trail: Home > Devices > Enroll devices > Enrollment Status Page > HomeLab Enrollment Status Page. Below the breadcrumb is a search bar and a navigation menu with 'Overview', 'Manage', and 'Properties' (the active tab). The 'Properties' section is divided into three main areas: Basics, Settings, and Assignments. The 'Basics' section shows the Name as 'HomeLab Enrollment Status Page' and the Description as 'Darren's Lab - continue at your own risk!'. The 'Settings' section contains a list of configuration options with Yes/No/All values. The 'Assignments' section shows 'Included groups' as 'Windows10\_Autopilot'.

Section	Property	Value
Basics	Name	HomeLab Enrollment Status Page
	Description	Darren's Lab - continue at your own risk!
Settings	Show app and profile configuration progress	Yes
	Show an error when installation takes longer than specified number of minutes	60
	Show custom message when time limit error occurs	Yes
	Error message	Installation exceeded the time limit set by your organization. Please try again or contact your IT support person for help.
	Allow users to collect logs about installation errors	Yes
	Only show page to devices provisioned by out-of-box experience (OOBE)	Yes
	Block device use until all apps and profiles are installed	Yes
	Allow users to reset device if installation error occurs	Yes
	Allow users to use device if installation error occurs	No
	Block device use until these required apps are installed if they are assigned to the user/device	All
Assignments	Included groups	Windows10_Autopilot

- Show app and profile configuration progress
- Block until device and user are configured
- Control behaviour with timeouts, error messages, recovery options



# Configuration and Security Profiles



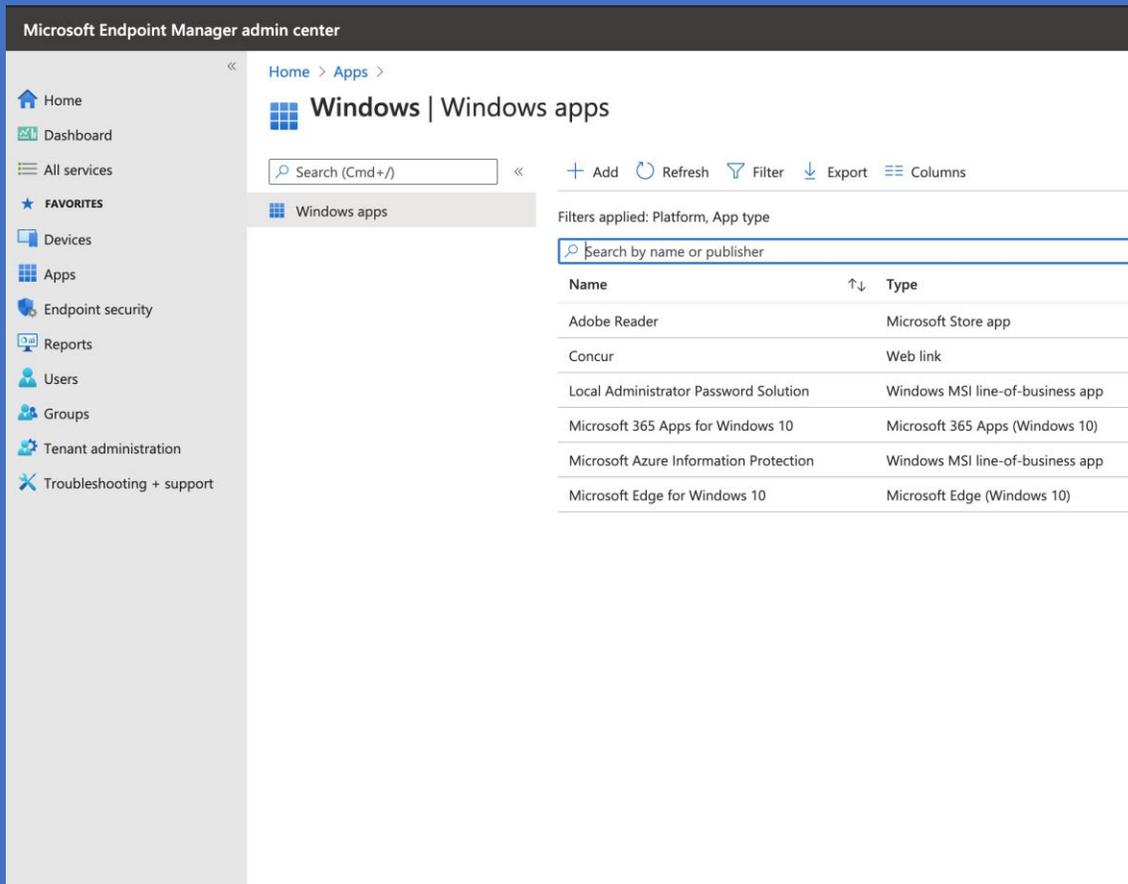
The screenshot shows the Microsoft Endpoint Manager admin center interface. The left sidebar contains navigation options: Home, Dashboard, All services, FAVORITES, Devices, Apps, Endpoint security (selected), Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled 'Endpoint security | Security baselines' and includes a search bar, an overview section with links for Overview, All devices, Security baselines (selected), and Security tasks, and a 'Manage' section with links for Antivirus, Disk encryption, Firewall, Endpoint detection and response, Attack surface reduction, Account protection, Device compliance, Conditional access, and Setup. A table titled 'Security Baselines' is displayed with the following data:

Security Baselines	Associated Profiles
Windows 10 Security Baseline	1
Microsoft Defender ATP Baseline	1
Microsoft Edge Baseline	1

- Configuration policies
- Security baselines
- Attack Surface Reduction
- Conditional Access
- Compliance

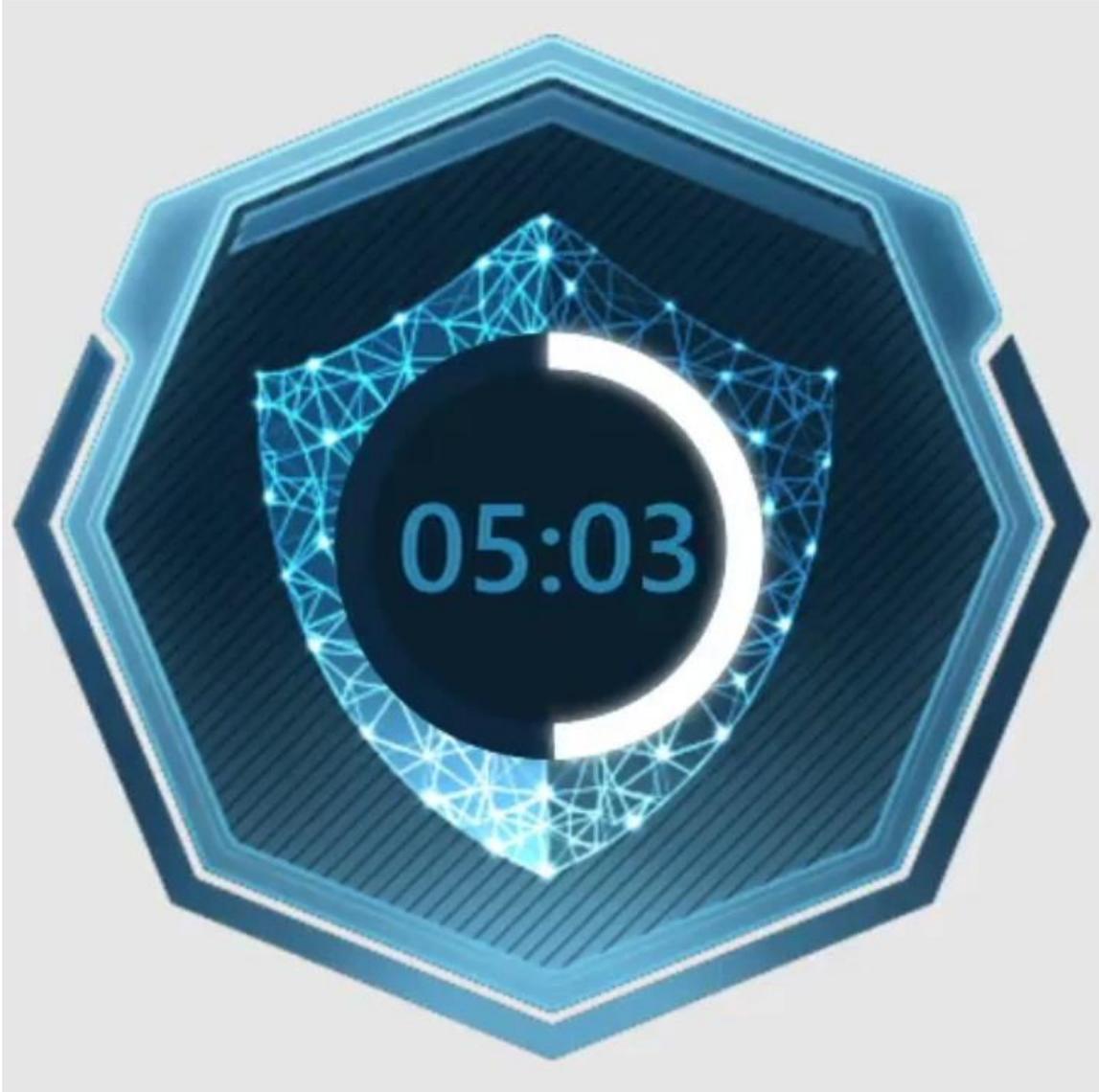


# Deploy Applications



- Quickly and easily deploy apps
- Windows (Store, Win32, Web links and Line of Business MSI)
- iOS
- Android
- MacOS
- Including App Protection Policies

5 Minute break





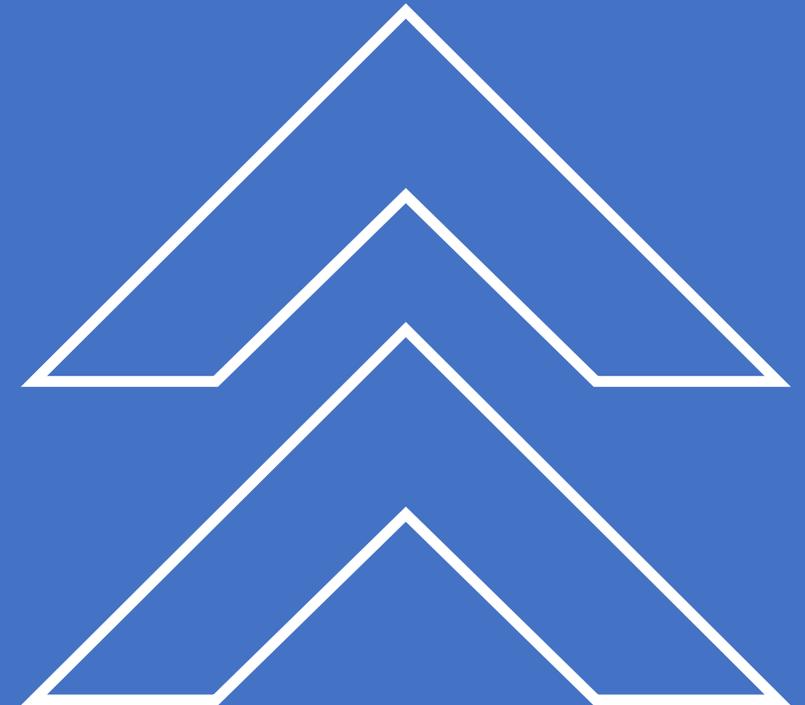
DICKER  
DATA



# Intune & Security

# What is Intune?

- 100% cloud-based Mobile Device and Application Management (MDM & MAM)
- App and Data protection
- Android, Android Enterprise, iOS/iPadOS, MacOS, and Windows
- Integrates with other services, including Entra ID, mobile threat defenders, ADMX templates, Win32 and custom LOB apps, and more.





# Best practice security, at your fingertips

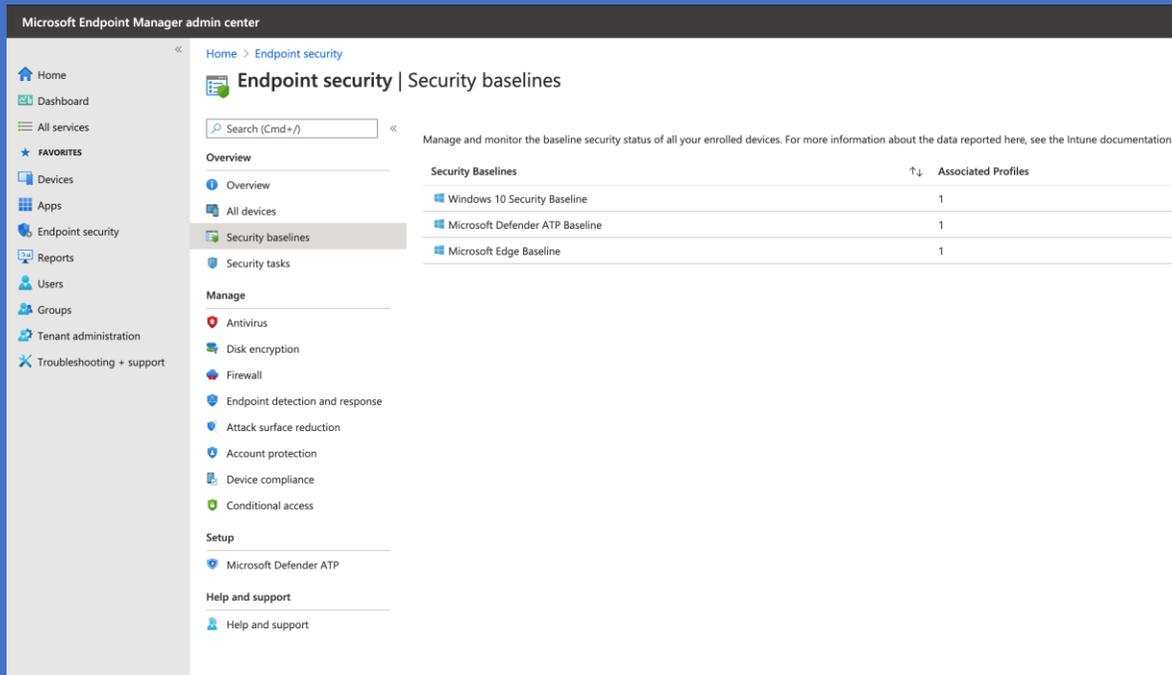
ASCEND

The screenshot displays the Microsoft Endpoint Manager admin center. The left-hand navigation pane includes sections for Home, Dashboard, All services, FAVORITES, and various management tools like Devices, Apps, Endpoint security (highlighted with a red box), Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled 'Endpoint security | Overview' and features a search bar and a 'Manage' section with a list of security settings: Antivirus, Disk encryption, Firewall, Endpoint detection and response, Attack surface reduction, Account protection, Device compliance, and Conditional access. The 'Setup' section shows 'Microsoft Defender ATP' is enabled. The main content area is divided into three columns: 'Protect and secure devices from one place' (Microsoft recommended security settings), 'Simplified security policies' (a list of categories like Antivirus, Disk encryption, Firewall, etc.), and 'Remediate endpoint weaknesses' (a list of tasks like Microsoft ATP connector enabled).

- Minimal and consistent interface reduces complexity and collates related configuration
- Baseline policies will capture 95%+ of your requirements
- Defender for Endpoints includes Recommended Configuration and more



# Microsoft Security Baselines & Attack Surface Reduction



- Microsoft recommended configurations
- Updated periodically to defend against new threats
- Combined with Attack Surface Reduction rules
- Office 365 baseline coming soon
- Familiarity and testing are paramount



# Application Protection and Control

ASCEND

The screenshot displays the Microsoft Endpoint Manager admin center interface. The left-hand navigation pane includes sections for Home, Dashboard, All services, FAVORITES, and various management tools like Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled 'Intune App Protection | Properties' and is categorized under 'Windows Information Protection'. It features a search bar and a 'Manage' section with 'Properties' selected. The configuration is organized into several sections: 'Basics Edit' (Name: Windows Information Protection, Description: --, Enrollment state: With enrollment), 'Targeted apps Edit' (Protected apps: 24 selected, Exempt apps: 0 selected), 'Required settings Edit' (Windows Information Protection mode: Block, Corporate identity: intune.mobi), and 'Advanced settings Edit' (Network perimeter, Network boundary: 0 Configured, Enterprise Proxy Servers list is authoritative: Off, Enterprise IP Ranges list is authoritative: Off, Data protection: Upload a Data Recovery Agent (DRA) certificate: Not configured, Prevent corporate data from being accessed: Off).

- Define sanctioned applications – Defender Application Control (aka AppLocker)
- Unsanctioned applications cannot be executed, including installers – even for administrators!
- Control the applications that can interact with company data
- Protect storing of corporate data

# App Protection Policies (APP)



Multi-identity awareness

Targets corporate accounts, not personal and unmanaged



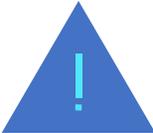
Conditional launch

Device health  
OS version  
App version/SDK  
Device model or manufacturer



Access requirements

PIN  
Biometrics  
Credentials  
Inactivity timers



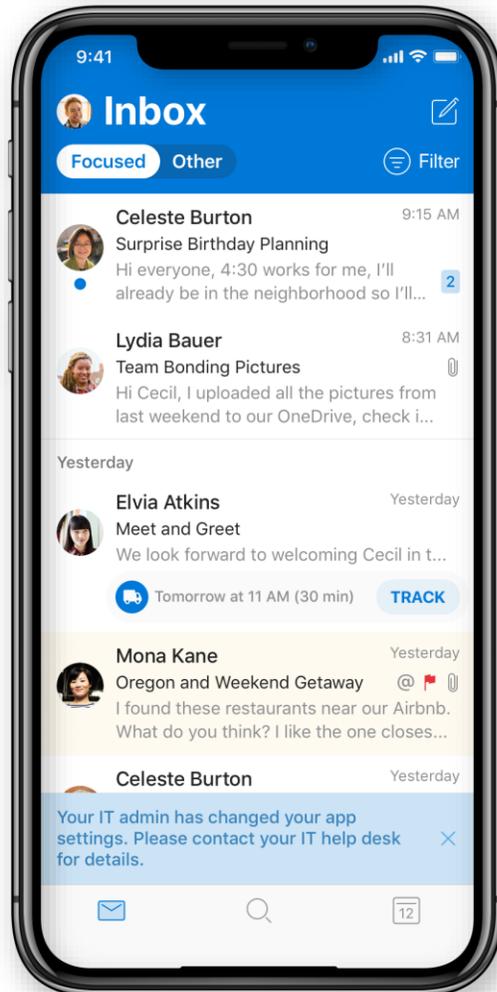
Data protection

Between apps  
Encryption  
Transfer web data  
Selective wipe

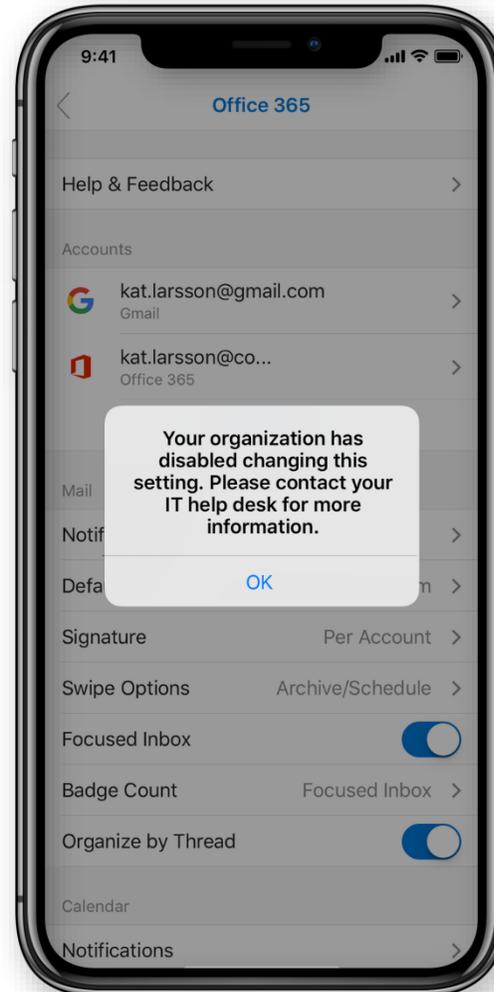
# General App Configuration Policy settings



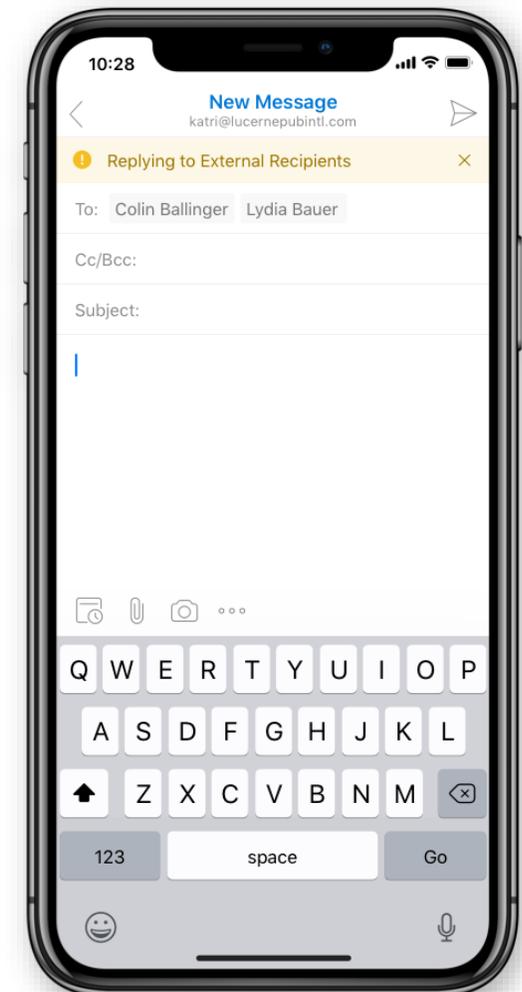
Focused Inbox



Contact Sync



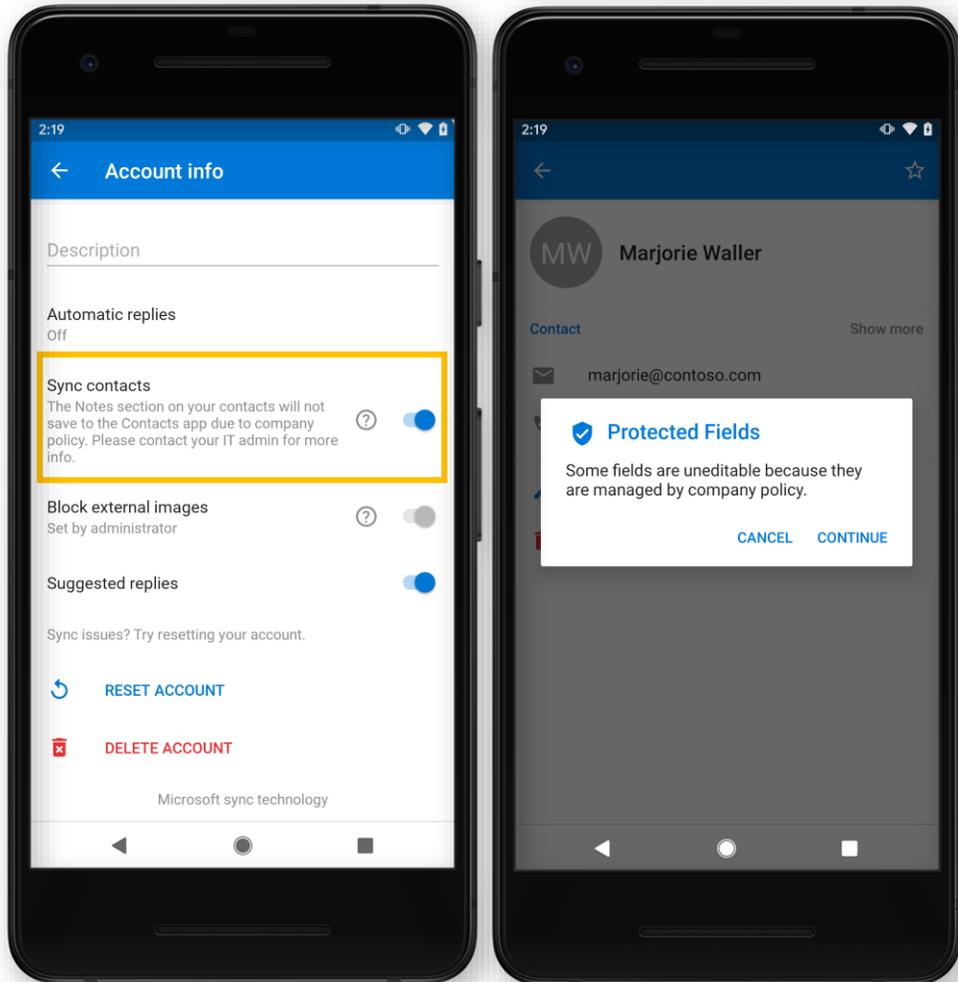
MailTips



# Data Protection App Configuration Policy settings



Limit Contact field export properties



Block wearables



User experience





# Group Policy Analytics



Microsoft Endpoint Manager admin center

Home > Devices > Test

Group Policy analytics (preview)

Refresh Filter Export Got feedback? Back

Search by Setting Name or MDM Support

Setting Name	Group Policy Setting Category	ADMX Support	MDM Support	Value	Min OS Version	Scope	CSP Name	CSP Mapping
Add Search Internet link to Start Menu	Start Menu and Taskbar	No	No	Enabled	0	User		
Allow users to enable online speech recog...	Control Panel/Regional and Language Opti...	No	Yes	Enabled	17755	Device	Policy	/Device/Vendor/MSFT/Poli...
Configure Automatic Updates/Configure a...	Windows Components/Windows Update	No	Yes	3 - Auto download an...	15063	Device	Policy	/Device/Vendor/MSFT/Poli...
Configure Automatic Updates/Every week	Windows Components/Windows Update	No	Yes	Enabled	15063	Device	Policy	/Device/Vendor/MSFT/Poli...
Configure Automatic Updates/First week o...	Windows Components/Windows Update	No	Yes	Disabled	15063	Device	Policy	/Device/Vendor/MSFT/Poli...
Configure Automatic Updates/Fourth week...	Windows Components/Windows Update	No	Yes	Disabled	15063	Device	Policy	/Device/Vendor/MSFT/Poli...
Configure Automatic Updates/Install durin...	Windows Components/Windows Update	No	Yes	Enabled	15063	Device	Policy	/Device/Vendor/MSFT/Poli...
Configure Automatic Updates/Install updat...	Windows Components/Windows Update	No	No	Disabled	0	Device		
Configure Automatic Updates/Scheduled L...	Windows Components/Windows Update	No	Yes	0 - Every day	15063	Device	Policy	/Device/Vendor/MSFT/Poli...
Configure Automatic Updates/Scheduled L...	Windows Components/Windows Update	No	Yes	03:00	15063	Device	Policy	/Device/Vendor/MSFT/Poli...
Configure Automatic Updates/Second wee...	Windows Components/Windows Update	No	Yes	Disabled	15063	Device	Policy	/Device/Vendor/MSFT/Poli...
Configure Automatic Updates/Third week ...	Windows Components/Windows Update	No	Yes	Disabled	15063	Device	Policy	/Device/Vendor/MSFT/Poli...
Disable context menus in the Start Menu	Start Menu and Taskbar	No	Yes	Enabled	17130	Device	Policy	/Device/Vendor/MSFT/Poli...
DNS servers/IP addresses:	Network/DNS Client	No	No	192.168.10.1	0	Device		
DNS suffix search list/DNS Suffixes:	Network/DNS Client	No	No	home.local	0	Device		
Java permissions/Java permissions	Windows Components/Internet Explorer/n...	Yes	Yes	131072	17134	Device	Policy	/Device/Vendor/MSFT/Poli...
Pin Apps to Start when installed	Start Menu and Taskbar	No	No	Disabled	0	Device		
Prevent bypassing SmartScreen Filter warni...	Windows Components/Internet Explorer	Yes	Yes	Enabled	15063	Device	Policy	/Device/Vendor/MSFT/Poli...
Prohibit use of Internet Connection Sharin...	Network/Network Connections	No	Yes	Enabled	17130	Device	Policy	/Device/Vendor/MSFT/Poli...
Remove "Recently added" list from Start M...	Start Menu and Taskbar	No	Yes	Enabled	17130	Device	Policy	/Device/Vendor/MSFT/Poli...

Showing 1 to 20 of 30 records

< Previous Page 1 of 2 Next >

- Analyze existing Group Policies
- The service directs you to the precise related configuration item in Intune
- CSP – Configuration Service Provider is the Intune equivalent of a Group Policy
- Custom CSPs can be created where required



# Compliance in a click

ASCEND

Microsoft Endpoint Manager admin center

Home > Reports

## Reports | Device compliance

Search (Cmd+/)

Overview

Refresh

Last refreshed on: 08/01/2021, 10:25:50

### Device compliance

Compliant: 8 devices | Noncompliant: 0 devices | Managed by ConfigMgr: 0 devices | Total: 8 devices

Device compliance status	
Status	Devices
<strong>Compliant</strong>	
Compliant	8
In grace period	0
<strong>Noncompliant</strong>	
Not compliant	0
Not evaluated	0
<strong>Other</strong>	
Managed by Configuration Manager	0

- Quickly and easily see device compliance
- Conditional Access policies based on device health or security risk posture
- Risk based compliance and Conditional Access via Defender for Endpoint
- Require Windows 10 minimum version, firewall, anti-virus, real-time protection

# Azure AD Join Device Demonstration





DICKER  
DATA



# Thank you

Microsoft Modern Work Team

MARCH 2024



# Resources



The following resources are supplied to aid in learning about Endpoint Manager (Intune and Autopilot) as part of the Dicker Data Centre of Excellence (COE)

## Autopilot FAQ

<https://docs.microsoft.com/en-us/mem/autopilot/autopilot-faq>

## Autopilot Overview including How-to Guides

<https://docs.microsoft.com/en-us/mem/autopilot/windows-autopilot>

## Autopilot Specific Documentation

<https://docs.microsoft.com/en-us/mem/autopilot/enrollment-autopilot>

## Intune Documentation

<https://docs.microsoft.com/en-us/mem/intune/>

## Video Enablement (highly recommended) - The Steve and Adam Show – covers everything Intune!

<https://www.youtube.com/watch?v=OkeUN-tdfgs>

## Official (free & paid) Microsoft MS-102 Learning Paths and certification information

<https://learn.microsoft.com/en-us/credentials/certifications/exams/ms-102/>

## Microsoft MS-102 Exam Reference Book (including Kindle for ~\$55 AUD).

The structure of this book is excellent and will be used to provide the structure in the MS-102 exam preparation COE enablement sessions

<https://www.amazon.com.au/Exam-Ref-MS-102-Microsoft-Administrator/dp/0138199469>

## M365 for Partners Training Resources

<https://www.microsoft.com/microsoft-365/partners/training?filters=sales-fundamentals>

