Microsoft Intune

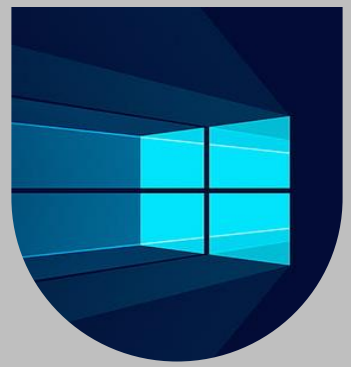
Ted Zhang

Morning & Afternoon sessions

Morning Session	Introductions & Learning Pathways Microsoft Intune & Autopilot Intune Design fundamentals
Afternoon Session	Intune Policy & Application Management Endpoint Security

Today's focus

Project-driven



Windows device

Autopilot deployment with pre-provisioning

Consulting Mindset

Microsoft Priorities

Copilot	Empower productivity and innovation with AI-driven Copilot solutions.
Security	Strengthen protection of data, users, and infrastructure across all platforms.
Migration	Enable seamless migration to modern Microsoft cloud services for enhanced efficiency.

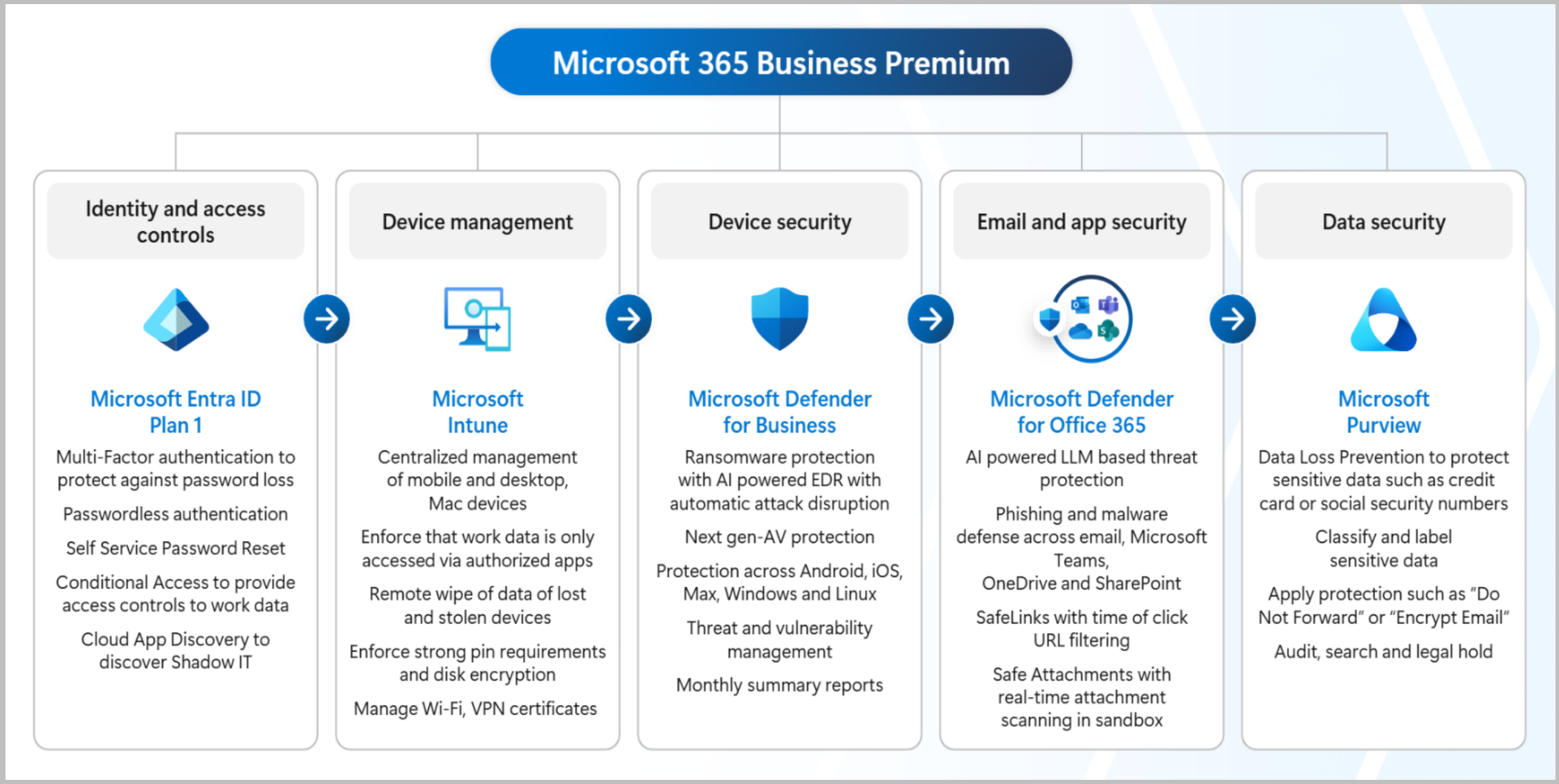
CIS controls and Essential 8

CIS Control	CIS Safeguard	Asset Class	Security Function	Title	Description	IG1	IG2	IG3
1				Inventory and Control of Enterprise Assets	*Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.*			
1	1.1	Devices	Identify	Establish and Maintain Detailed Enterprise Asset Inventory	Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.	x	x	x

Essential 8

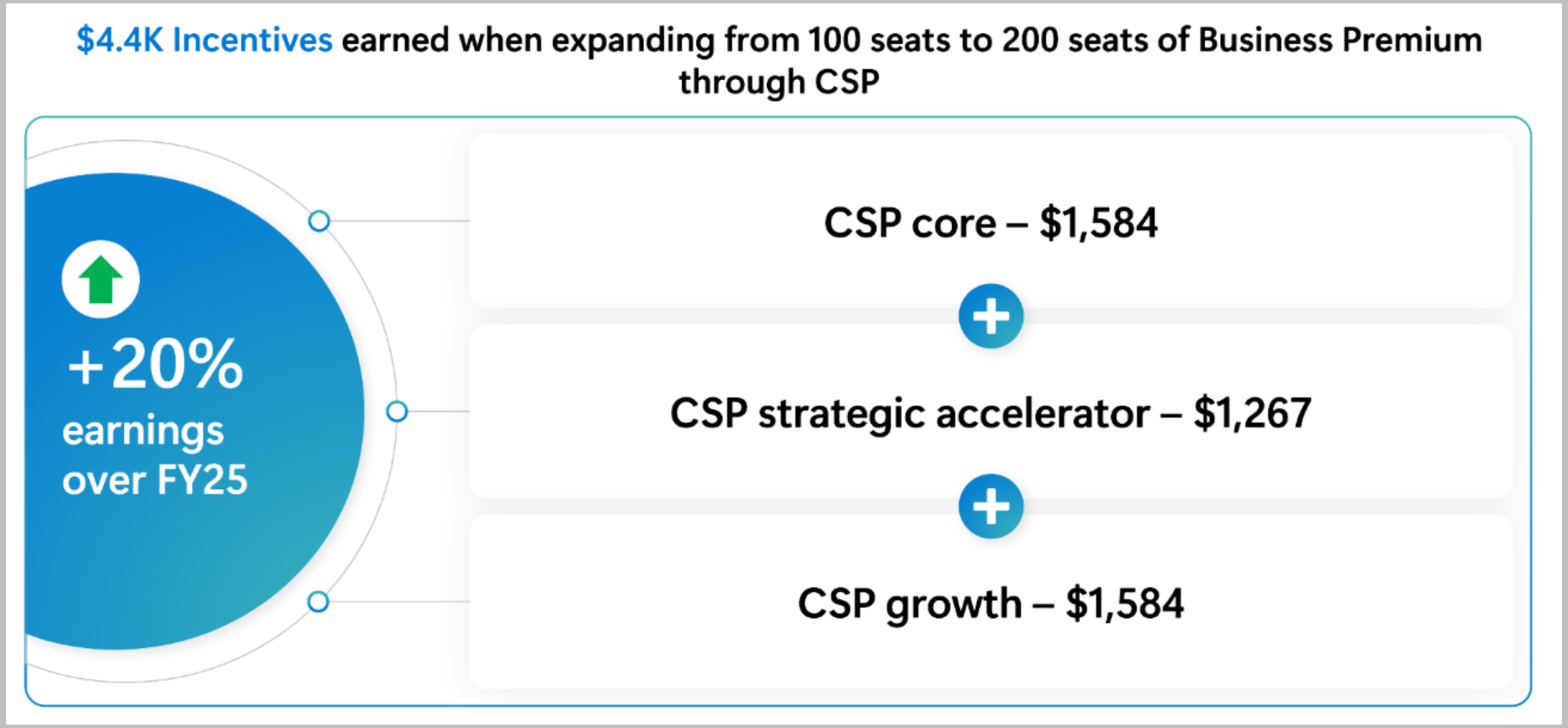
- Application Control
- Patch Applications
- Configure Microsoft Office Macro Settings
- User Application Hardening
- Restrict Administrative Privileges
- Patch Operating Systems
- Multi-Factor Authentication (MFA)
- Regular Backups

Licensing



https://learn.microsoft.com/en-us/microsoft-365/business-premium/m365bp-overview?view=o365-worldwide

Microsoft Incentives



Microsoft 365 CSP incentive - indirect reseller

Requirement -

- 25 points minimum
- $25K USD 12-month revenue

Measure and Reward

Incentives are based on billed revenue and calculated in accordance to billing cadence.

M365 CSP levers	Rate	Maximum incentive earning opportunity
M365 CSP Core	3.75%	$93,750
M365 CSP Global Strategic Product Accelerator – Tier 1 (Business Premium, M365 E3)	*Innovate and Balance countries**: 3.00%	$75,000*
	*Scale countries***: 4.00%	$100,000**
M365 CSP Global Strategic Product Accelerator – Tier 2 (M365 E5, Copilot)	7.00%	$175,000
M365 CSP Global Calling and Conference PSTN Accelerator	20.00%	Not applicable
M365 CSP Growth Accelerator*	7.50%	$187,500

IMPORTANT: October 1, 2025 to November 30, 2025 will be calculated and paid under FY26 partner eligibility, levers, and rates. Earnings will be paid by January 15, 2026 per incentive launch payment SLA here.

	Business Applications CSP incentives	Azure CSP incentives			Modern Work and Security CSP incentives	
	Solutions Partner for Business Applications	Solutions Partner for Data & AI (Azure)	Solutions Partner for Digital & App Innovation (Azure)	Solutions Partner for Infrastructure (Azure)	Solutions Partner for Modern Work	Solutions Partner for Security
Category: Performance	15pts	30pts	30pts	30pts	20pts	20pts
Skilling	35pts	40pts	40pts	40pts	25pts	40pts
Customer success	50pts	30pts	30pts	30pts	55pts	40pts

Learning pathways & Certification

MS-900 & SC-900 & AZ-900

MD-102/SC-300

- https://learn.microsoft.com/en-us/credentials/certifications/modern-desktop/?practice-assessment-type=certification

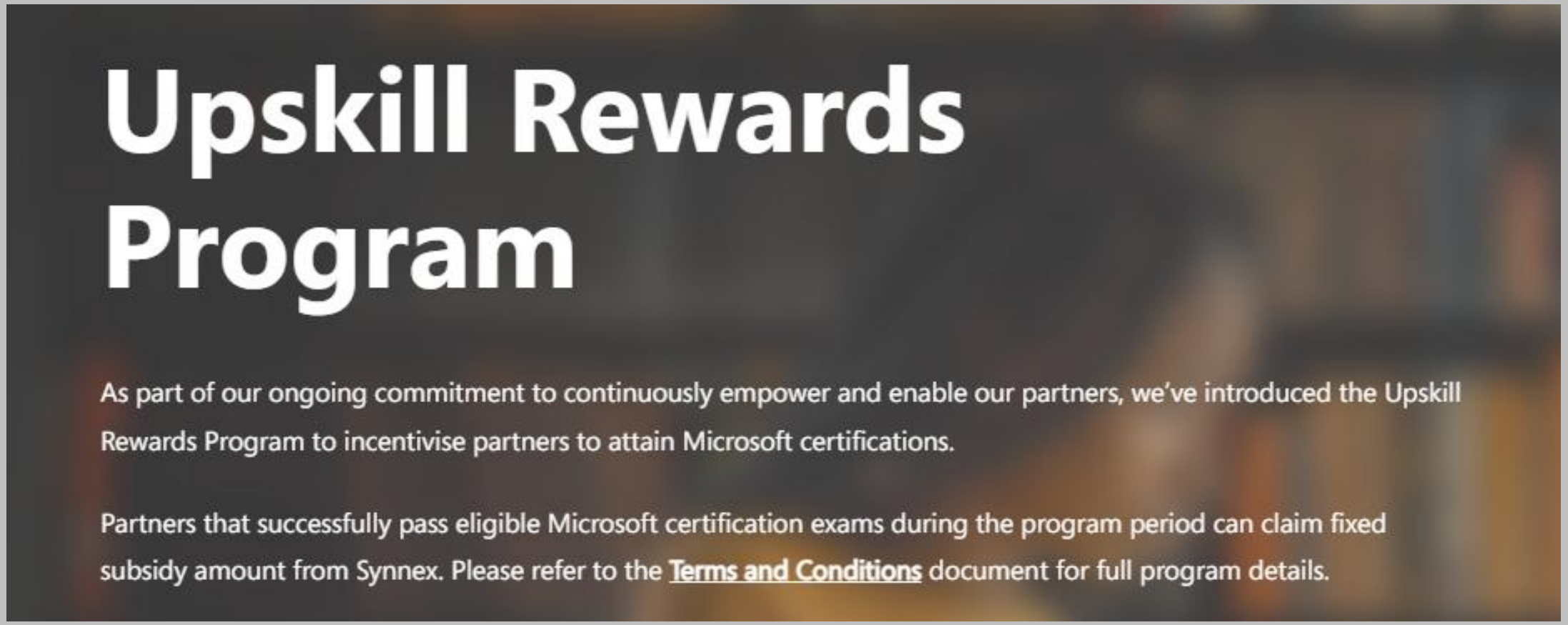
MS-102

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

SC-200

SYNNEX Incentives and webinars

https://csp.synnex.com.au/



Current Promotions:

Metallica Experience: Score tickets to the Metallica M72 world tour with Synnex CSP!

Microsoft 365 Accelerators: Earn up to $8,000 rebate on eligible Microsoft 365 products.

Copilot Accelerators:
Category 1: Get 100% subsidy for first 3 months when you purchase up to 49 new seats of M365 Copilot.
Category 2: Get 100% subsidy for 10 seats per partner for the first 3 months when you add 50 or more new seats of M365 Copilot.

Azure rewards:
Power Boost: Get 80% off your first month PAYG Azure invoice for a new customer.
Power Build: Get up to $15,000 in subsidy for leveraging CSP professional services.

Small Business Big Security: Earn up to $1,000 rebate when you transact in M365 E5 Security add-on.

Upskill Rewards Program: Get your exam fee subsidised when you successfully complete an eligible Microsoft certification exam.

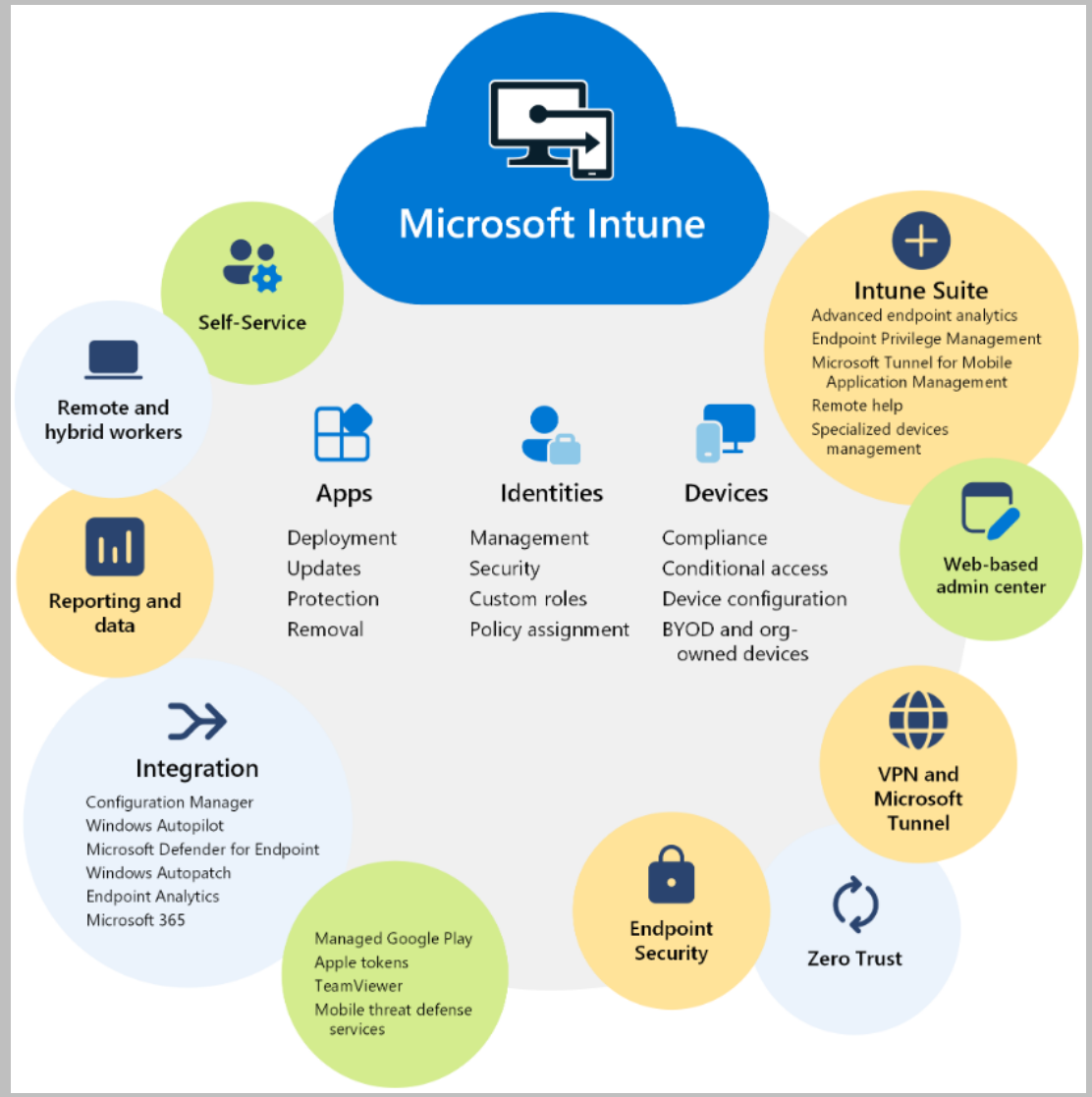
Ready to unlock these incentives?
Register your deals through Synnex CSP today

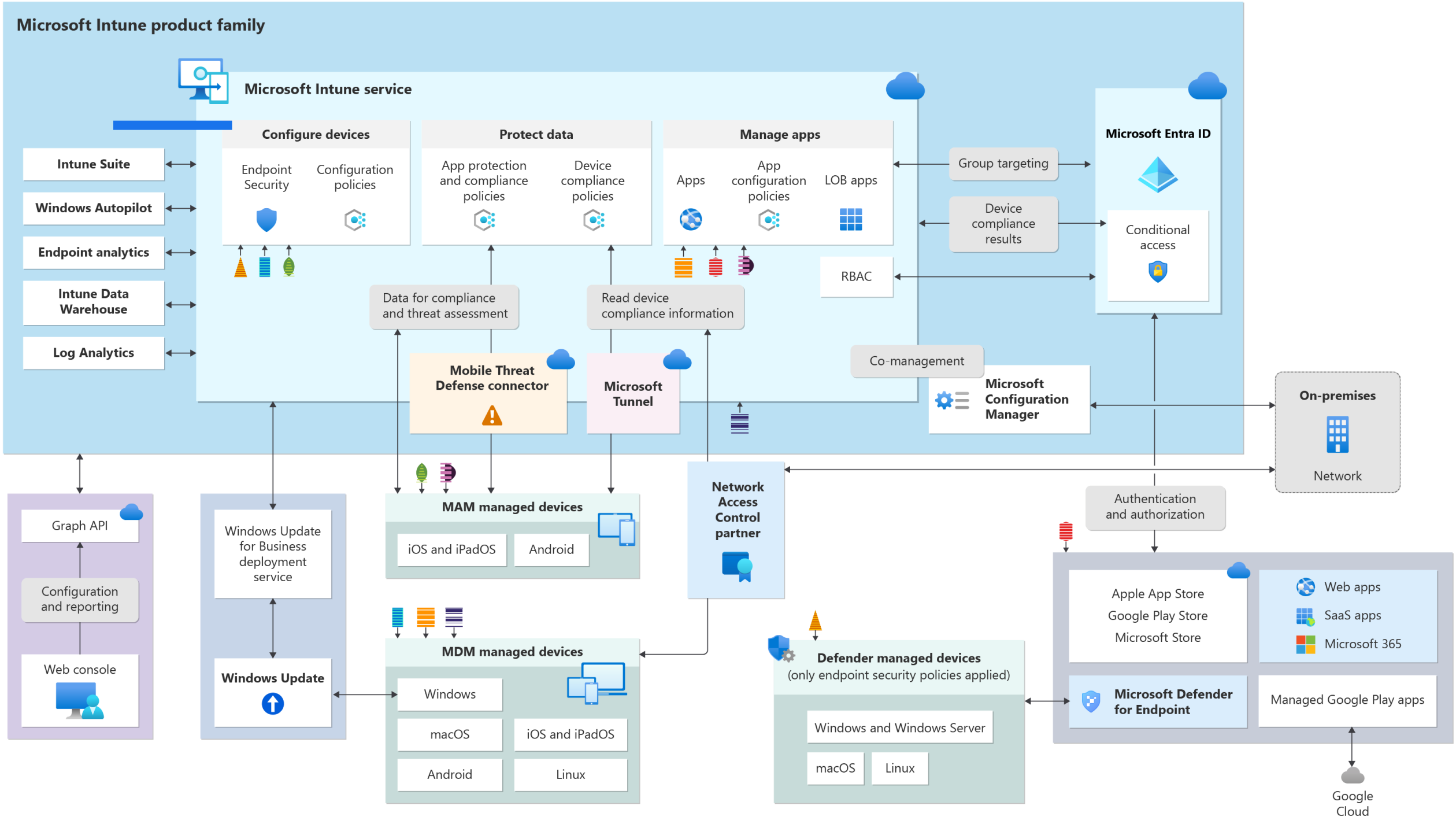
*Terms and conditions apply.

Overview of Microsoft Intune

Microsoft Intune is a **cloud-based endpoint management solution**.

- **App deployment** – Push Win32, Microsoft Store, web, and mobile apps to devices.
- **Configuration policies** – Define rules and controls for device health, security, and compliance.
- **Conditional Access integration** – Restrict access to Microsoft 365 and other resources based on compliance.
- **Endpoint security** – Configure security baselines, antivirus (Defender), BitLocker, firewall, and more.
- **Windows Autopilot integration** – Automate Windows device provisioning and setup.
- **Remote actions** – Wipe, reset, lock, locate, or retire devices remotely.




Microsoft Intune product family
Microsoft Intune service
Intune Suite
Windows Autopilot
Endpoint analytics
Intune Data Warehouse
Log Analytics
Configure devices
Endpoint Security
Configuration policies
Protect data
App protection and compliance policies
Device compliance policies
Manage apps
Apps
App configuration policies
LOB apps
Group targeting
Device compliance results
RBAC
Microsoft Entra ID
Conditional access
Data for compliance and threat assessment
Read device compliance information
Mobile Threat Defense connector
Microsoft Tunnel
Co-management
Microsoft Configuration Manager
On-premises
Network
Graph API
Configuration and reporting
Web console
Windows Update for Business deployment service
Windows Update
MAM managed devices
iOS and iPadOS
Android
Network Access Control partner
Authentication and authorization
MDM managed devices
Windows
macOS
iOS and iPadOS
Android
Linux
Defender managed devices
(only endpoint security policies applied)
Windows and Windows Server
macOS
Linux
Apple App Store
Google Play Store
Microsoft Store
Web apps
SaaS apps
Microsoft 365
Microsoft Defender for Endpoint
Managed Google Play apps
Google Cloud

Intune - Pros

Cloud native

No on-premise infrastructure required

Microsoft Integration

Integrated with Entra ID, Defender and Microsoft Purview

Security & Compliance

Intune security policies and Microsoft Defender

Scalability and Autopilot

Intune is suitable for SMBs and large corporations

Intune - Cons

Join type

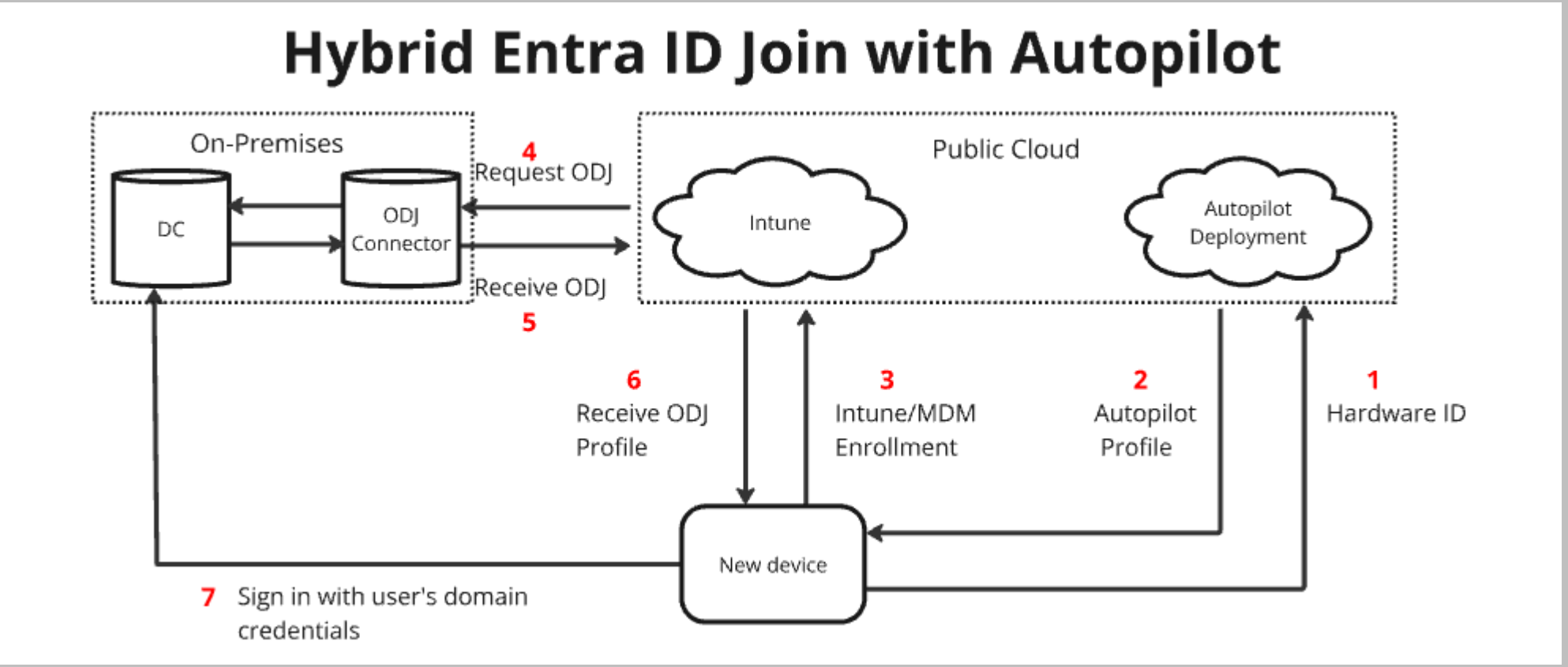
- Hybrid Join
- Entra ID Join
- Entra ID registered
- Co-managed with SCCM

Hybrid Join Setup

Actions	Details
Install and configure Intune Connector	Microsoft Intune uses the on-premises Intune connector to generate a machine object in Entra ID. The connector acts as a bridge between on-premises AD and Entra ID.
Create Managed Service Account (June 2025)	Create msDs-ManagedServiceAccount objects in the Managed Service Accounts container
OU Delegation	Configure the MSA to allow creating objects in OUs
Manually change device name if required	Hybrid join does not support customized naming convention for devices, only prefix
Create Domain join profile in Intune	Domain join profile is used to contact on-prem domain

Enrollment for Microsoft Entra hybrid joined devices - Windows Autopilot | Microsoft Learn

Hybrid Join workflow (Simplified)



Benefits of Hybrid Join

Access to On-Prem Resources

File shares, legacy apps, on-prem printers

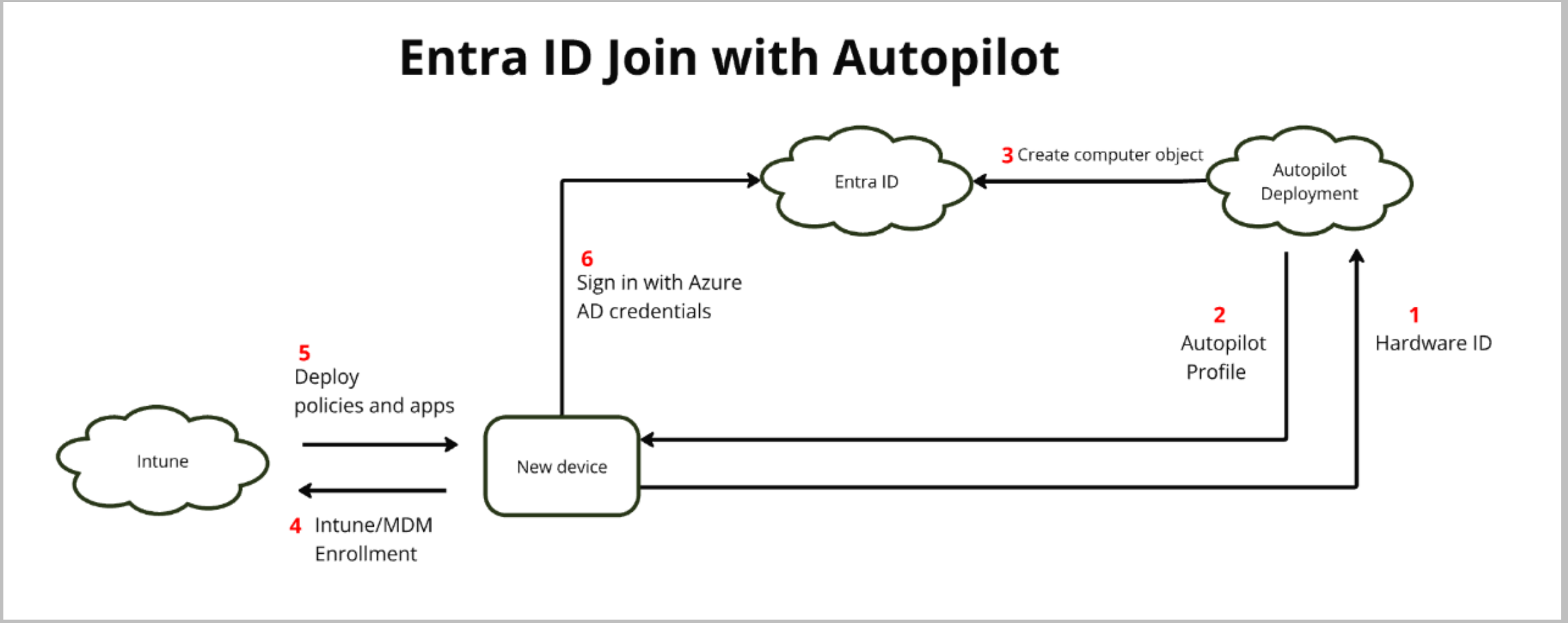
Group Policy

Full GPO support

Certificate (via On-prem Certificate Authority)

Device certificates for Wi-Fi, VPN, etc., via on-prem Certificate Authority

Entra ID Join workflow



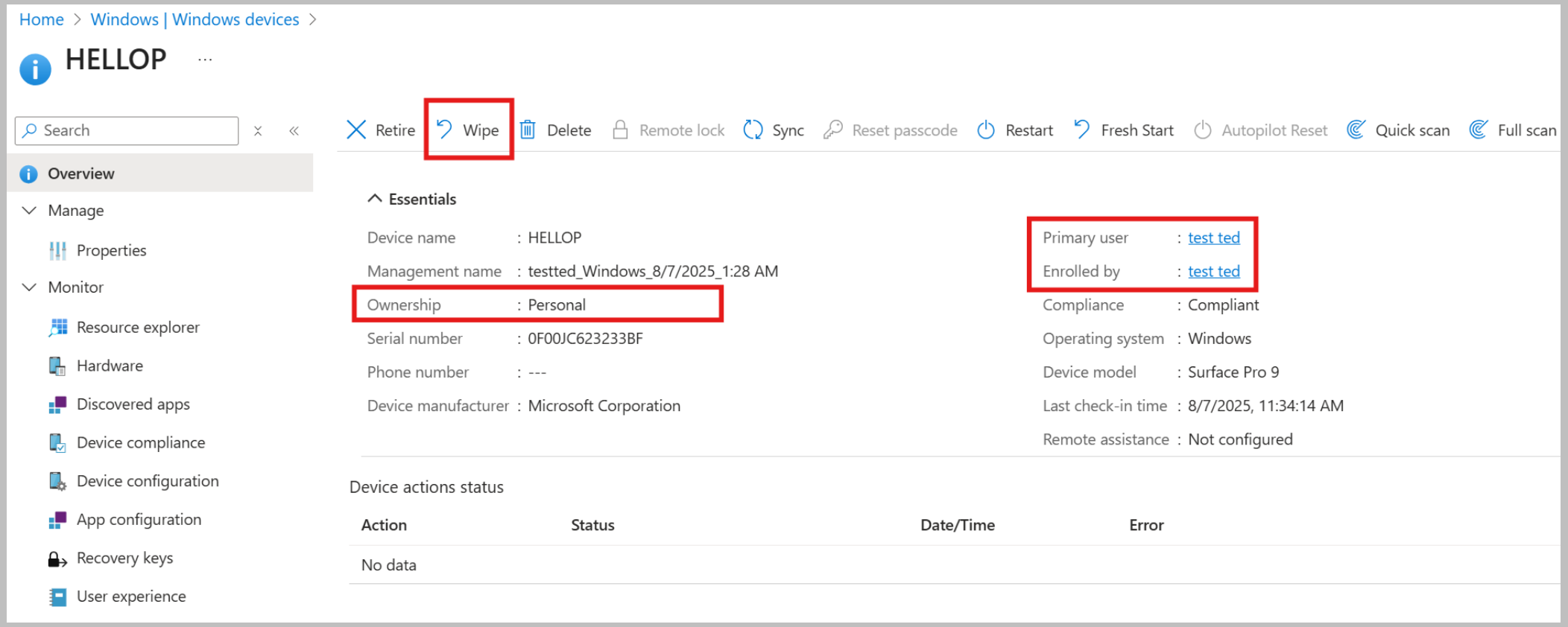
Hybrid Join vs Entra ID Join

- Entra ID Join is highly recommended by Microsoft, it not only reduces on-premises overheads but also you can control everything in single pane of glass. Entra ID join is easy to set up and avoid potential policy conflictions

- Hybrid Join requires on-premises infrastructure and line of sight to on-premises Domain controller is required for user authentication. Device naming convention is not as flexible as Entra ID Join.

Entra ID Register

Designed for BYOD device. However, even the device is only Entra ID registered, Intune can still "fully manage" the device.



https://learn.microsoft.com/en-us/entra/identity/devices/concept-device-registration

Join type – quick recap

	Hybrid Join	Entra ID Join	Entra ID registered
On-prem AD required	YES	NO	NO
Company device	YES	YES	NO
Managed by Intune	YES	YES	YES

If Entra ID registered is bad, what if my clients have requirement to use employees' personal device to access company data?

Windows 365

Use case –

- For employees with own PC
- Contractors or temp employee
- Shared device

Benefits -

- Data compliance for international company
- Scale up and down
- Easy to set up and fixed monthly pay

Enrolment options

- Hybrid join via GPO
- Autopilot
- End User enrolment via Access work or school in settings
- Bulk enrolment with provisioning package

https://learn.microsoft.com/en-us/intune/intune-service/fundamentals/deployment-guide-enrollment-windows#co-management-enrollment

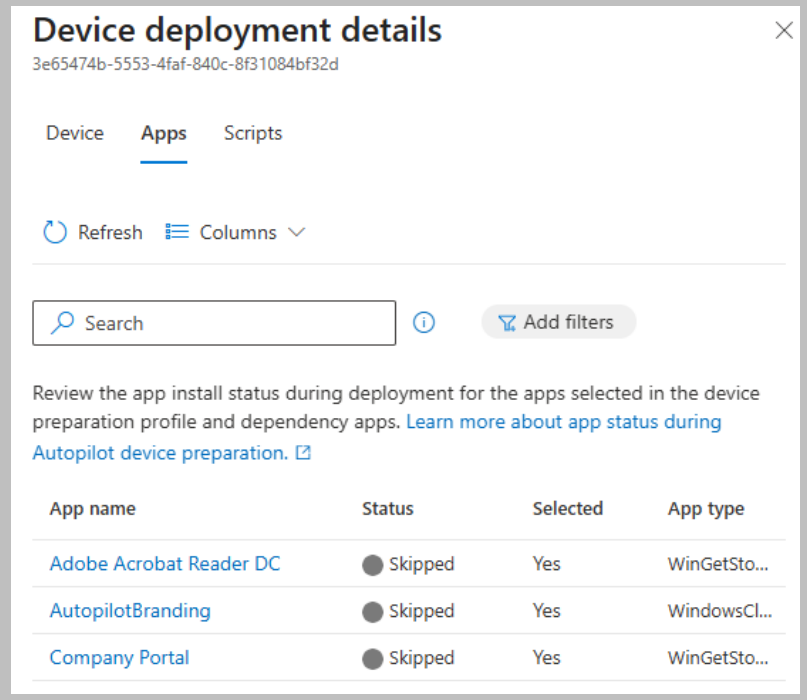
Enrolment type

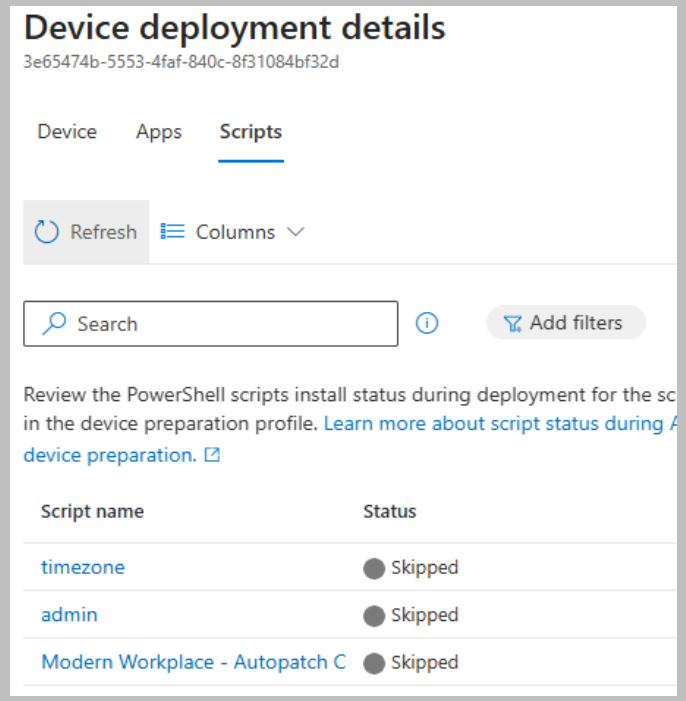
Element	Self-service setup	Windows Autopilot	Bulk enrollment
Require user interaction to set up	Yes	Yes	No
Require IT effort	No	Yes	Yes
Applicable flows	OOBE & Settings	OOBE only	OOBE only
Local admin rights to primary user	Yes, by default	Configurable	No
Require device OEM support	No	Yes	No
Supported versions	1511+	1709+	1703+

https://learn.microsoft.com/en-us/entra/identity/devices/device-join-plan

Autopilot device preparation

Autopilot device preparation is a simplified version of Intune Autopilot, it is relatively easy to configure but there are just too many drawbacks, such as does not support pre-provisioning, apps are skipped if managed installer is in use, does not support group tag.





Known issue: Windows Autopilot device preparation with Win32 apps and managed installer policy | Microsoft Community Hub

Autopilot device preparation vs Autopilot

Supported modes	• User-driven. • Automatic.	• User-driven. • Pre-provisioned. • Self-deploying. • Existing devices.
Join types supported	• Microsoft Entra join.	• Microsoft Entra join. • Microsoft Entra hybrid join.
Device registration required?	No.	Yes.
What do admins need to configure?	• Windows Autopilot device preparation policy. • Device security group with **Intune Provisioning Client** as owner.	• Windows Autopilot deployment profile. • Enrollment Status Page (ESP).
What configurations can be delivered during provisioning?	• Device-based only during the out-of-box experience (OOBE). • Up to 10 essential applications (line-of-business (LOB), Win32, Microsoft Store, Microsoft 365). • Up to 10 essential PowerShell scripts.	• Device-based during device ESP. • User-based during user ESP. • Up to 100 applications.

https://learn.microsoft.com/en-us/autopilot/device-preparation/compare#windows-autopilot-device-preparation-vs-windows-autopilot

Autopilot & Intune

Consider Autopilot and Intune are 2 different phases – Autopilot register and Intune enrolment

Autopilot is for ...	Intune is for ...
Upload hardware hash to register device to the tenant	Apply policies, install required apps and scripts
Assign device to an Entra ID group based on Tag	Integration with Microsoft defender and Purview
Customize Out of box experience (OOBE)	
Enable Pre-provisioning	

Autopilot with pre-provisioning/whiteglove

Autopilot Scenarios

·User Driven Deployment with Enrollment Status Page disabled

New device ordered → End user → Log in and start working

Apps and configurations will be deployed in background when user logs in

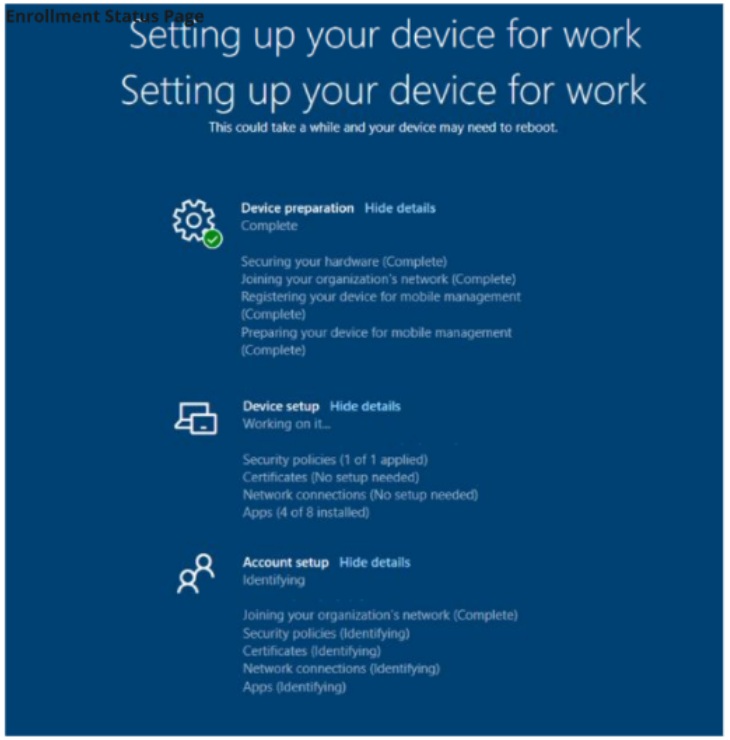
·User Driven Deployment without white glove

New device ordered → End user or IT Support → Wait for applications and policies to be deployed to device → Log in and start working

·User Driven Deployment with white glove

New device ordered → BC build team → Wait for applications and policies to be deployed → End user or IT Support → Log in and start working

1. A valid Intune license must be assigned before user logs into device
2. A pre-login VPN must be configured for initial sign-in if user works from home



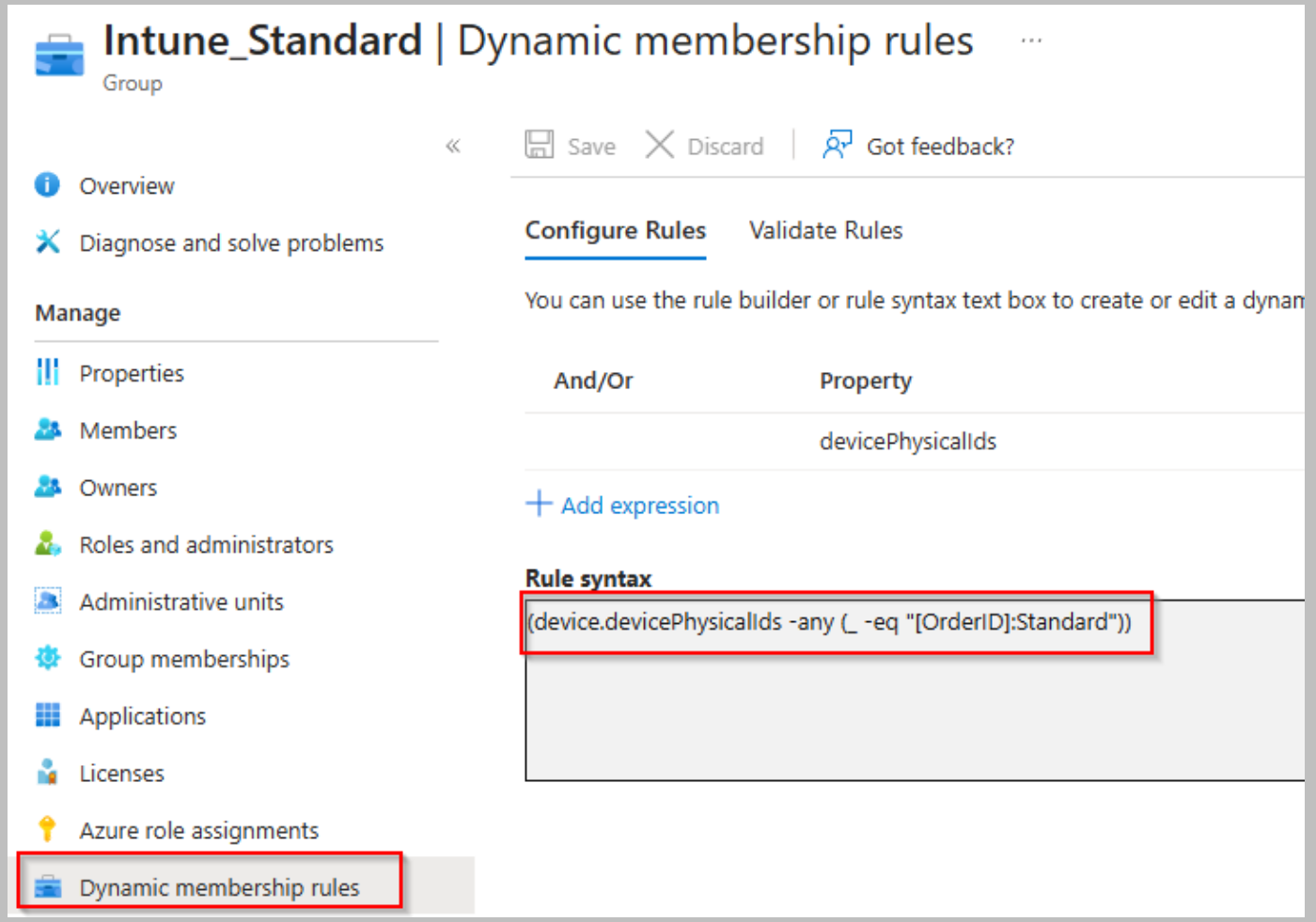
Hardware hash

For Autopilot to work, we need to upload something called hardware hash. Once uploaded, the device is bound to the Intune tenant.

Hardware hash is not required for Autopilot device preparation, instead, you need to upload Corporate device identifiers if you block BYOD.

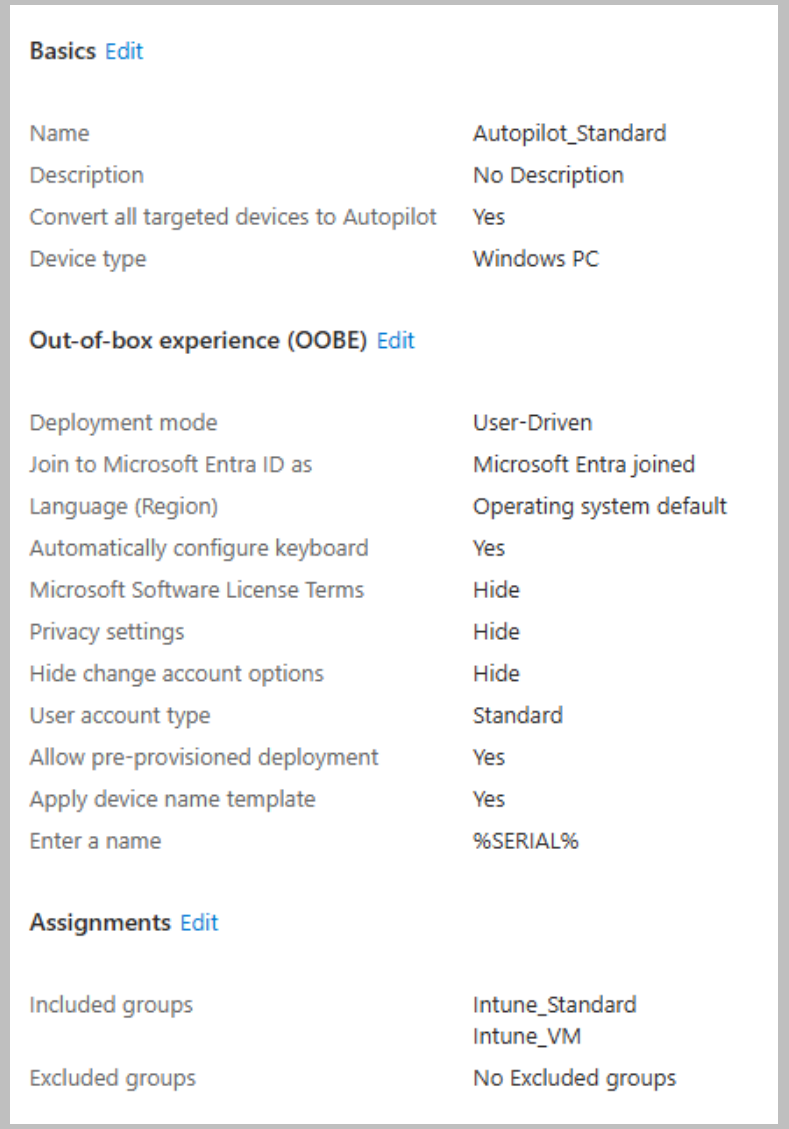
Group tag

- Group tag is assigned during Autopilot register process, it is mentioned in the script.
- Group tag is important, it tells which Entra ID group the device is going to join.
- Policies, apps and scripts assigned to this Entra ID group will be installed/applied during Pre-provisioning phase.
- You can use different group tags for different departments/personas



Deployment profile

- Configure OOBE
- Define join type
- Enable pre-provisioning



Basics Edit

Name	Autopilot_Standard
Description	No Description
Convert all targeted devices to Autopilot	Yes
Device type	Windows PC

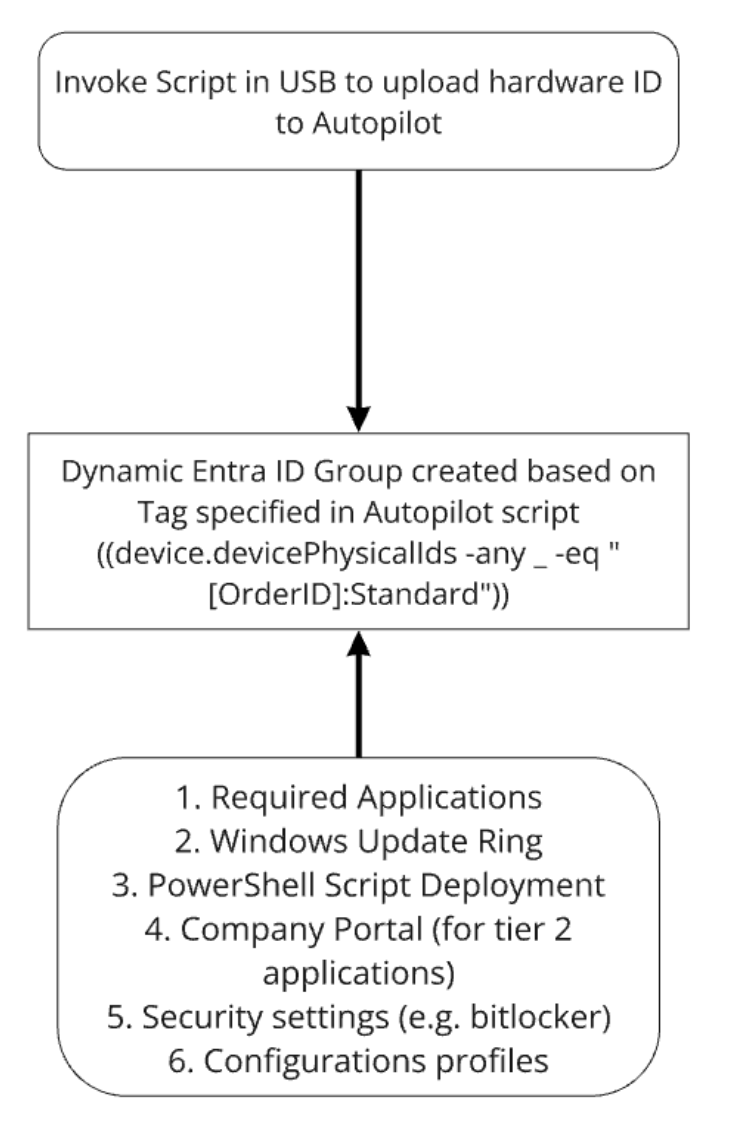
Out-of-box experience (OOBE) Edit

Deployment mode	User-Driven
Join to Microsoft Entra ID as	Microsoft Entra joined
Language (Region)	Operating system default
Automatically configure keyboard	Yes
Microsoft Software License Terms	Hide
Privacy settings	Hide
Hide change account options	Hide
User account type	Standard
Allow pre-provisioned deployment	Yes
Apply device name template	Yes
Enter a name	%SERIAL%

Assignments Edit

Included groups	Intune_Standard Intune_VM
Excluded groups	No Excluded groups

Enrolment flow with Autopilot



1. Start laptop and plug in USB with script
2. Press shift + F10 or go to sysprep to run the script
3. Enter tag (deployment profile) and/or device name
4. Wait for the device to be registered (upload hardware hash) in Autopilot portal
5. From Region Selection screen, initiate Autopilot by pressing Windows key 5 times then finish whiteglove/pre-provisioning process to install scripts, apps, policies, etc.
6. Shutdown device and send it customer

Demo - Upload hardware hash

- The script is recommended and recognized by Microsoft -

  https://learn.microsoft.com/en-us/autopilot/add-devices#powershell

- You can specify the computer name, tag then pass them to script, there are many other parameters you can use, the main purpose for the script is to upload hardware hash to tenant.

Troubleshoot

- Install-Script -Name Get-AutopilotDiagnostics –Force
- Application logs
- Microsoft logs

Microsoft Frequent Asked Questions

- https://learn.microsoft.com/en-us/autopilot/troubleshooting-faq
- https://learn.microsoft.com/en-us/troubleshoot/mem/intune/device-enrollment/understand-troubleshoot-esp

Building a house...

Intune design fundamentals

- Statement of Work
- Initial discovery
- High-level
- Low-level (Architectural decisions)
- Design and Build
- Pilot
- Close
- Hypercare

Statement of Work

- Consultant may or may not be involved (Sales + Tech pre-sales/Consultant)
- Define what needs to be done, timeline, cost, etc.
- There are always minor changes in later stage and gaps , e.g. update ring is required but not mentioned in SoW, there are many granular control/build in Intune unlike other M365 project.
- How many hours are you going to spend on this project?
- Based on the size of the project – do you need a project manager to assist you?

Initial Discovery

- Have a checklist ready
- Understand customer's current process, e.g. how do they image devices, what's the pain point, how do they deploy applications, security requirements, etc.

Category	Item
Identity & User Information	Is Microsoft Entra ID already in use?
Identity & User Information	Is Hybrid Join, Entra Join, or both used?
Identity & User Information	Are users synced via Entra Connect?
Device Landscape	Types of devices used (Windows, macOS, iOS/iPadOS, Android)
Device Landscape	Ownership model: BYOD or corporate-owned?
Device Landscape	Any existing MDM/EMM solution (e.g. Workspace ONE, Jamf, MobileIron)?
Device Landscape	Device count for each OS
Device Landscape	Are devices domain-joined? Local admin access? GPO?
Apps & Software	Critical line-of-business (LOB) apps
Apps & Software	Any legacy apps requiring local domain authentication
Apps & Software	Microsoft 365 apps usage
Apps & Software	How are Apps deployed?
Apps & Software	License models for app (per-user, per-device, etc.)
Security Baseline	Is Microsoft Defender for Endpoint in use or planned?

High Level Design

- Ensure customer understands some fundamentals are irreversible, e.g. Hybrid join or Entra ID join
- Provides a clear understanding on what will be covered/built for this project.
- This protects us from "Why is this not included?"

11. Out of Scope

The following tasks are defined as 'Out of Scope' for [redacted] initial Scope of Works. These items can be included in-scope if requested, times will be updated to take additional work into consideration.

- Analysis of existing GPO's
  - [redacted]
- Setup or remediation of Always on VPN outside of Intune deployment profile
- Testing of Windows 11 Operating System feature or quality updates
- Third party software update management
  - [redacted]
- Remediation of any incompatible applications. Alternatives will be recommended where possible.
- Remediation of application settings provided
- Implementation of application whitelisting or blacklisting
  - Intune includes the ability to control applications through Intune policies, however specific deny or allow of applications are generally handled by an alternate fit for purpose utility.
- Any existing hardware modification

Architectural decisions

- Decides how configurations are configured in areas mentioned in SoW
- This protects us from "Why is it configured this way"
- This document also provides an estimate of the hours required for this project

16. OneDrive Known Folder Move (KFN)

Subject Area	OneDrive Configuration
Topic	Automatic redirection of Desktop, Pictures, and Documents folders to OneDrive. Leave this policy blank if GPO controls KFN configuration
Options	The following options will be considered: • OneDrive Known Folder Move (KFN) • None
Decision	**Configure this in Intune but make it disabled for now**
Comment	

17. End user Account Type

Subject Area	End user account type
Topic	Discussion on whether end user should have admin privilege or non-admin privilege
Options	The following options will be considered: • Admin privilege • Non-admin privilege
Decision	**Non-admin privilege**

18. Wallpaper

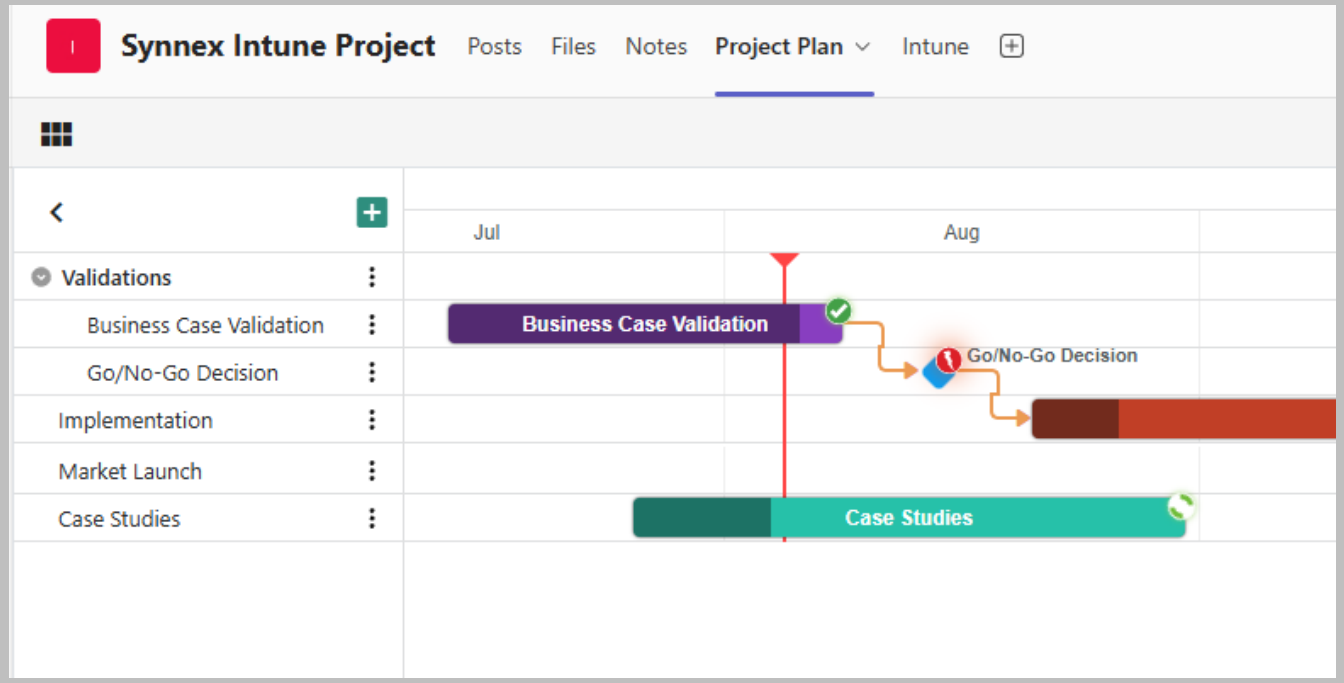
Subject Area	Wallpaper
Topic	Discussion on wallpaper
Options	The following options will be considered: • Wallpaper from GPO (No change required) • Wallpaper from Cloud storage (Cloud storage required) • Wallpaper from Script (Only available to new device build)
Decision	**Wallpaper from GPO (No change required)**

Design and Build

- Have a checklist
- There is no so called "best practices" as every environment is different. However, there are baselines you should almost always to deploy for clients.
- Reusability

https://github.com/jseerden/IntuneBackupAndRestore

GitHub - mtniehaus/AutopilotBranding

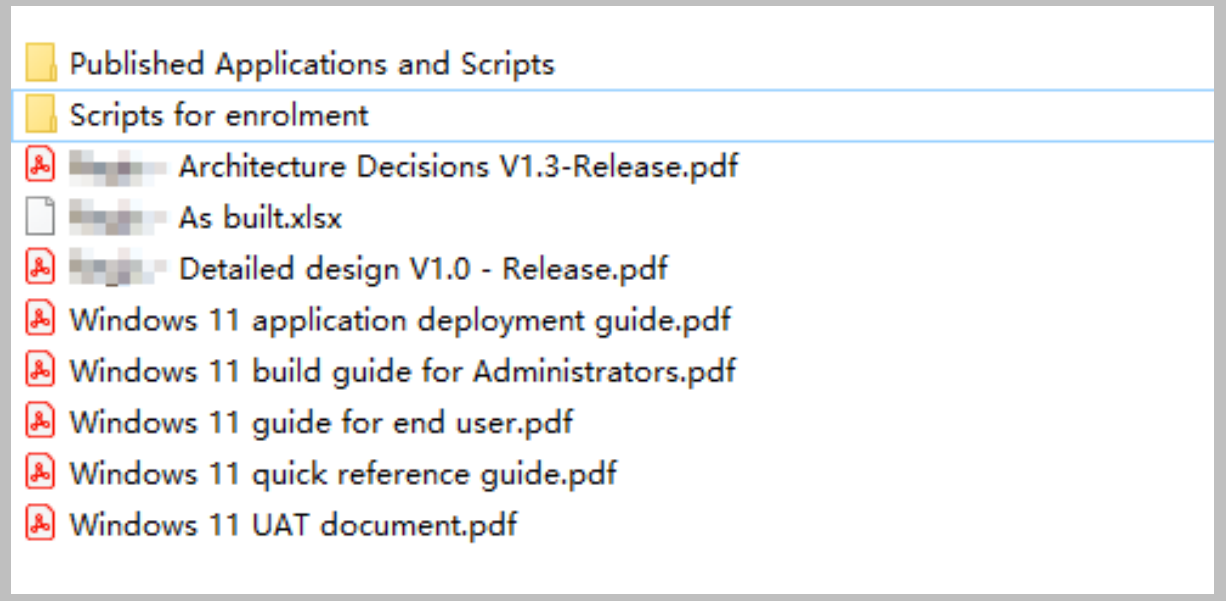


User Acceptance Test and hand-over

Test Outcomes

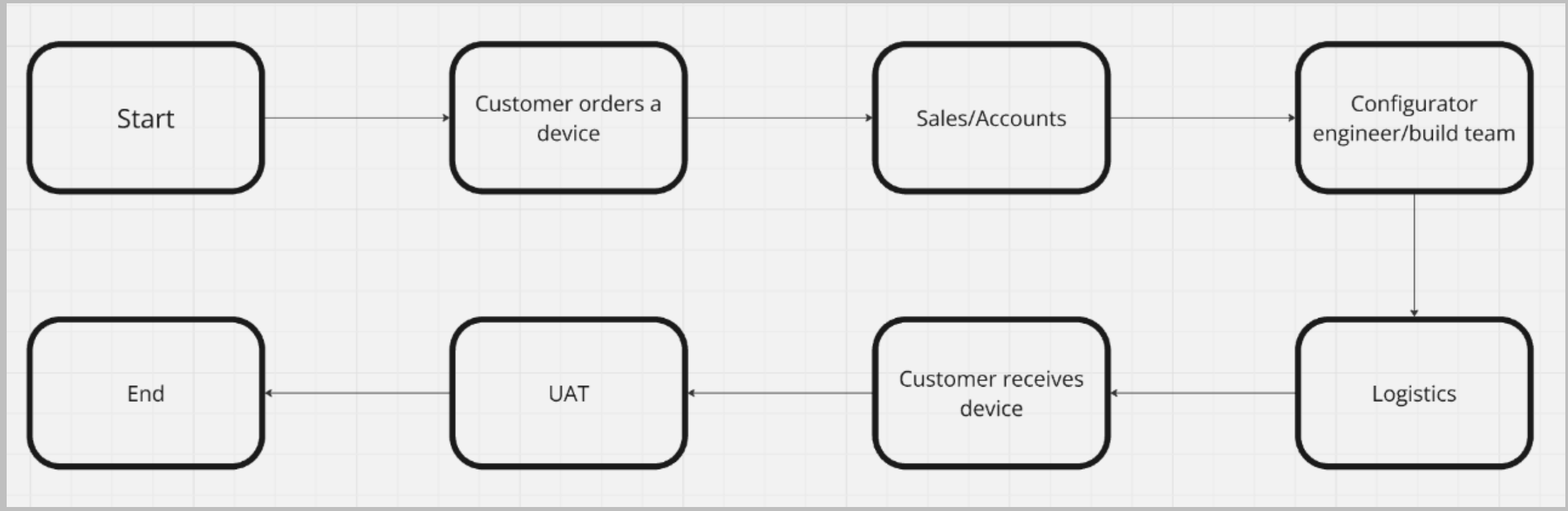
Checks to ensure device provisions and is configured and working as expected:

Test Stages	Outcome
Device registered in Autopilot	
Autopilot Pre-Provisioning succeeds	
Device enrolled in Intune	
Windows Login succeeds	
Company Portal is deployed	
Microsoft Teams is deployed	
Office suite is deployed	
Wi-Fi is connected	
Network Drives are mapped	
Printers are mapped	
Certificates are deployed	
Required apps are installed	
2nd tier app can be installed via Company Portal	



Pilot test

The pilot test includes whole device-built workflow, starts from "Customer requests a device".



Opportunity – Business Premium

Intune and Defender

- Autopilot
- EDR (Endpoint detection and response)
- ASR (Attack surface reduction) and WDAC (Windows Defender Application Control)
- LAPS (Local admin password solution)
- WHfB (Windows hello for business)
- WUfB (Windows update for business)

Purview

- DLP
- Copilot usage monitoring
- Labelling
- Retention Policy

Universal Print

- Cloud printing solution

Commercial Licenses	Jobs Per Month
Microsoft 365 E3, E5, Business Premium	100
Microsoft 365 F3	5
Windows 10 Enterprise E3, E5,	5
Universal Print (standalone)	5

Sharepoint & Exchange online

- OneDrive for Business data migration
- On-prem Exchange to Exchange online
- Sharepoint migration

Microsoft Defender E5 add-on

Security (MSSP)

- MDR/SOC (with Microsoft Experts)
- SIEM (Sentinel, Splunk, etc.)
- EASM (External Attack Surface Management)
- Defender for Cloud Apps (Apps)
- Defender for Cloud and Defender for Identity (Infrastructure)

Tool	Focus	Internal or External	Key Use
Defender EASM	External visibility	External	Discover and reduce internet-facing risks
Defender for Endpoint	Endpoint protection	Internal	Detect/respond to threats on devices
Microsoft Sentinel	SIEM/SOAR	Both	Aggregate and investigate alerts
Defender for Cloud	Cloud workload security	Internal (cloud infra)	Protect Azure, AWS, GCP resources
Defender for Cloud Apps	Cloud access control	Internal (cloud apps)	CASB for SaaS apps like M365, Salesforce

Onboarding/offboarding (Project)

- Entitlement management
- Access review
- API integration with HR system
- Power platform
- PIM & Risk-based CA

Security training (MSP)

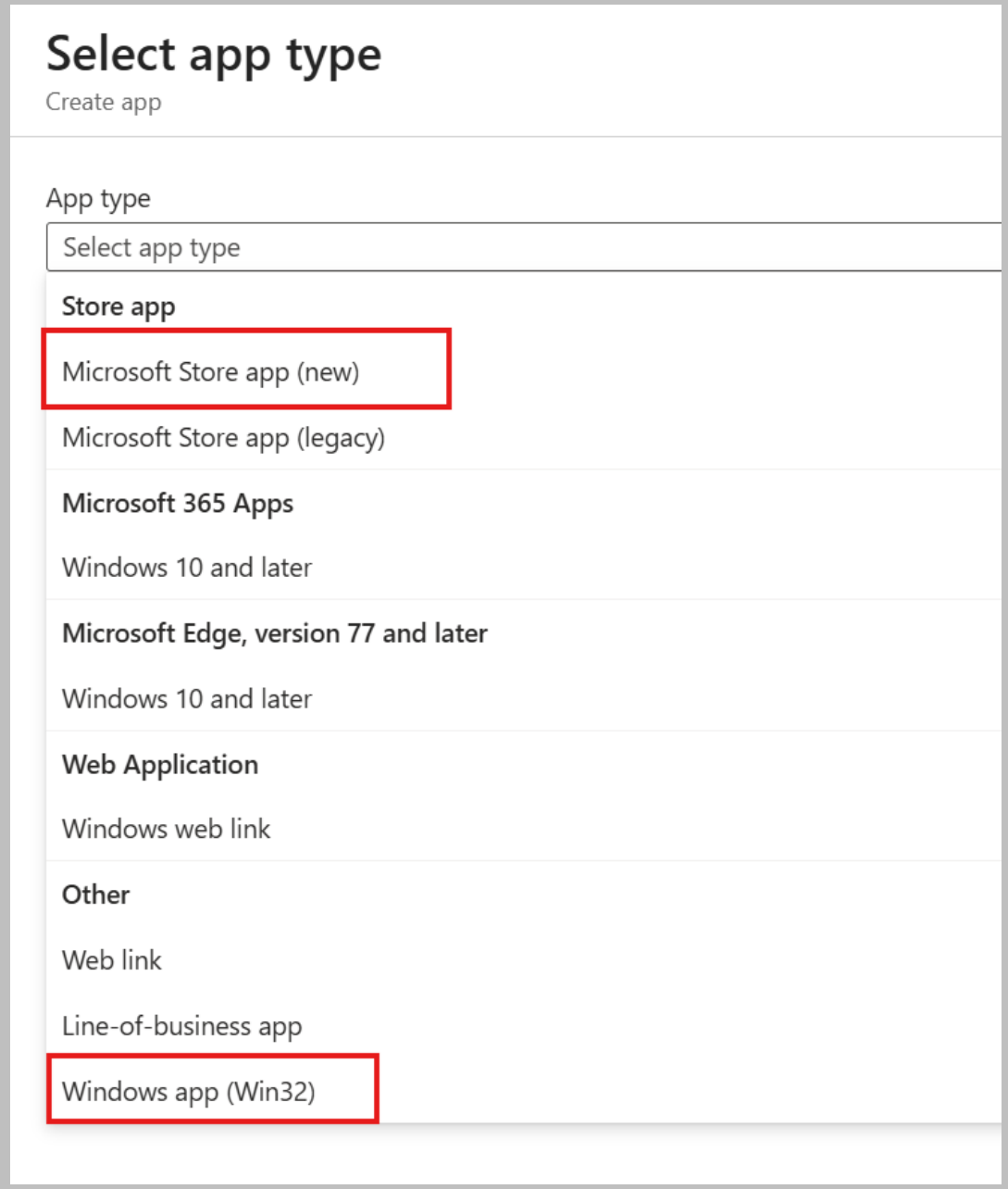
- Attack Simulation and Cyber-awareness training

Endpoint Management

- Application management
- Configuration profiles
- Windows hello for business
- Autopatch

App Management

- Microsoft Store app (new)
- Microsoft 365 Apps
- Windows app (Win32)
- Script (Win32)



Microsoft Store app (new)

Pros -

- **Trusted Source**
- **No Package Management**
- **Auto update by vendor**

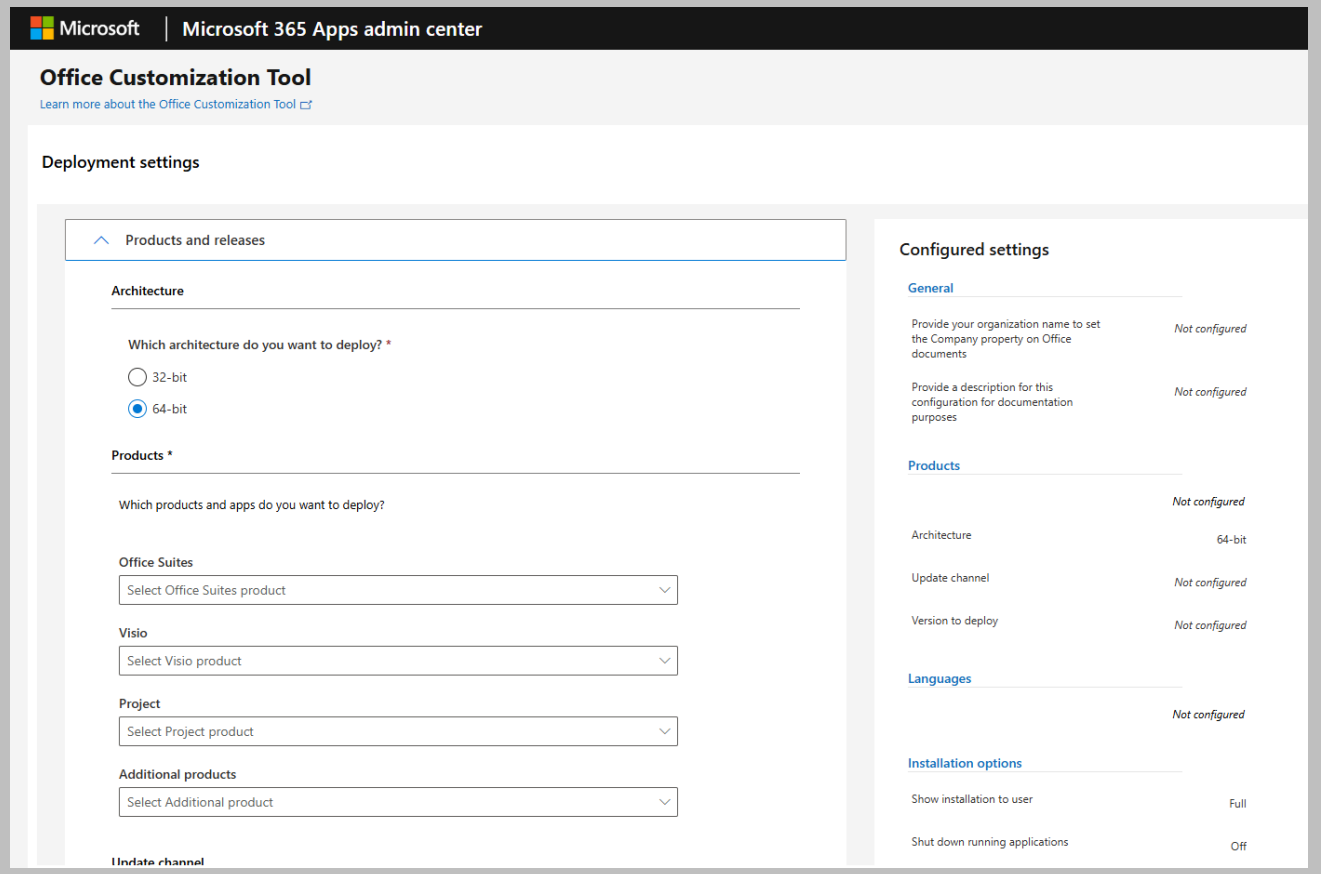
Cons -

- **Dependency on Store Availability**
- **Less control to zero control**

Microsoft 365 Apps

Recommended way to deploy office 365, including Outlook, Teams, Word etc.

You can use Office Customization tool to create an XML template for reuse capability and reliability – config.office.com



Line of Business app

A line-of-business (LOB) app is one that you add from an app installation file. This kind of app is typically written in-house.

> ⓘ **Important**
>
> When deploying Win32 apps using an installation file with the .msi extension (packaged in an .intunewin file using the Content Prep Tool), consider using Intune Management Extension. If you mix the installation of Win32 apps and line-of-business apps during Windows Autopilot enrollment, the app installation may fail as they both use the Trusted Installer service at the same time.
>
> Although Windows Autopilot doesn't support mixing of Win32 and line-of-business apps, Windows Autopilot device preparation does.

Windows app (Win32)

A **Windows app (Win32)** uses .exe or .msi installers. It also supports script packaging and pre-defined commands.

Pros	Cons
Wide compatibility	Packaging complexity
Flexible deployment	
Custom detection rules	
Full control over install behavior	
Mature tooling support	
Supports offline installation	
Scripts package	

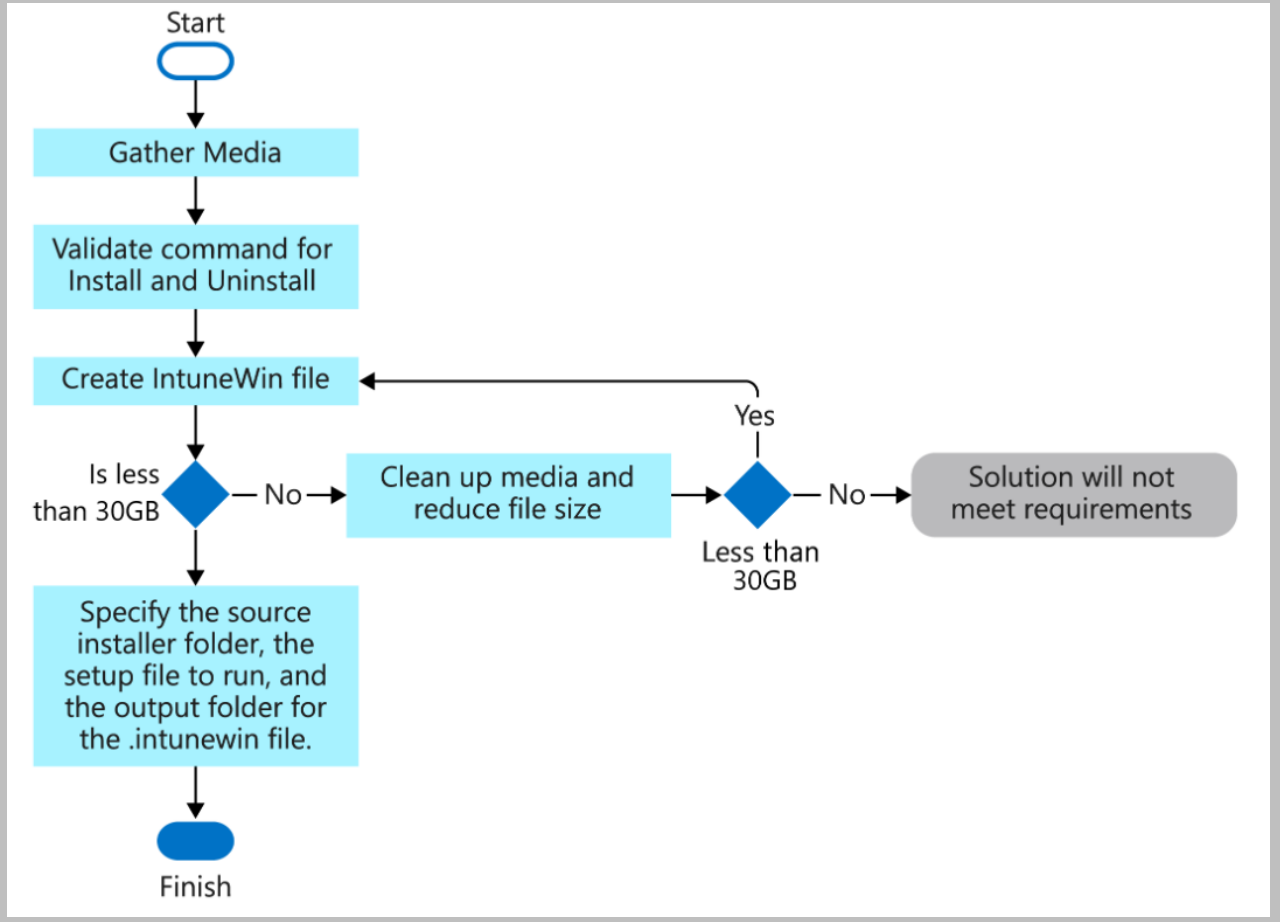
Win32 Content Prep Tool

This tool is used to convert the file you want to deploy to .Intunewin format. .msi file is highly recommended as .msi auto-populate many command lines.

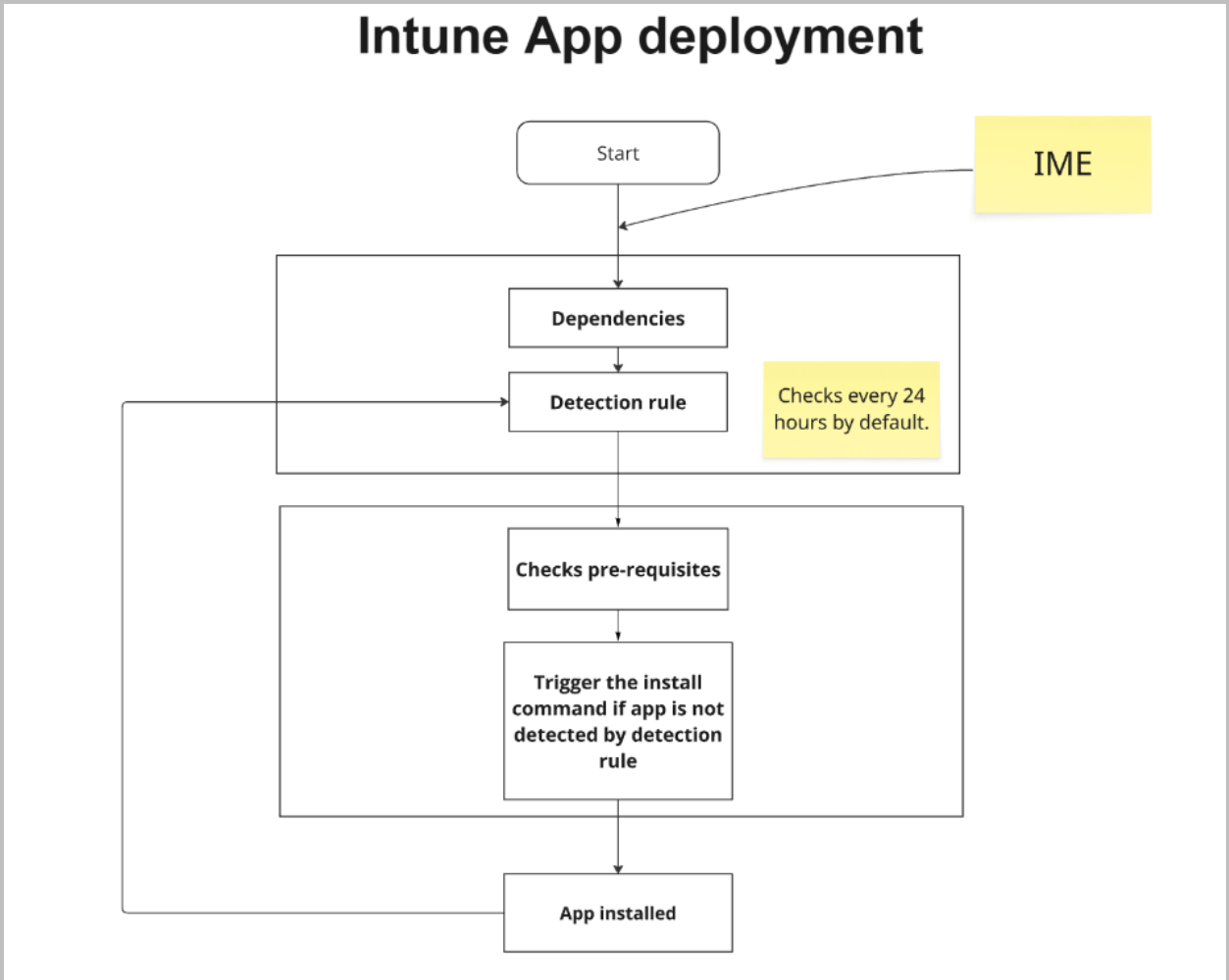
Why .msi?

- Designed for mass deployment
- Common switches supported by default including logging
- Default install and uninstall command
- Default detection rule

[Prepare a Win32 app to be uploaded to Microsoft Intune | Microsoft Learn]



Win32 App Deployment flow



https://learn.microsoft.com/en-us/troubleshoot/mem/intune/app-management/develop-deliver-working-win32-app-via-intune

Detection rule

There are 4 rule types -

- File-based detection
- MSI product code
- Registry Key
- Script

https://learn.microsoft.com/en-us/intune/intune-service/apps/apps-win32-add#step-4-detection-rules

Application Assignment

There are 3 assignment types for Windows device -

- Required
- Available for enrolled devices
- Uninstall

https://learn.microsoft.com/en-us/intune/intune-service/apps/apps-deploy

Question

You have a Win32 app in Microsoft Intune. The groups and assignments are:

- Group A contains User A and Device B.
- Group B contains Device A and User B.
- Group C contains Group A and Device A.

The app assignment is:

- Required → Group C
- Uninstall → Group A and Group B

Which users or devices will have the app installed?

A. User A
B. User B
C. Device A
D. Device B

App Update – Supersedence vs in-place update

Update type	Update description and details
In-place app update	• With an in-place app update, admin can only swap the app content, update the metadata, and change the detection and install commands. • Admin can't change any of the fields that aren't stored on the app with an in-place app update. For example, the admin can't modify targeting at the same time as an update. • Admin can only perform the in-place app update one app at a time.
Supersedence app update	• Admin can update an app in its entirety with a new set of configurations. • Admin can elect to send down an uninstall command to uninstall previous app versions. • Admin can update devices containing multiple app versions to the newest app version with one Supersedence configuration. The admin also maintains access to older version of the app.

https://learn.microsoft.com/en-us/intune/intune-service/apps/apps-win32-supersedence#understand-in-place-app-update-versus-supersedence-app-update

App Update – Winget

Winget, also known as the Windows Package Manager, is a command-line tool developed by Microsoft for discovering, installing, upgrading, and removing applications on Windows.

Winget is installed by default on Windows .... in user context :(

https://github.com/Romanitho/Winget-Install
https://learn.microsoft.com/en-us/windows/package-manager/winget/

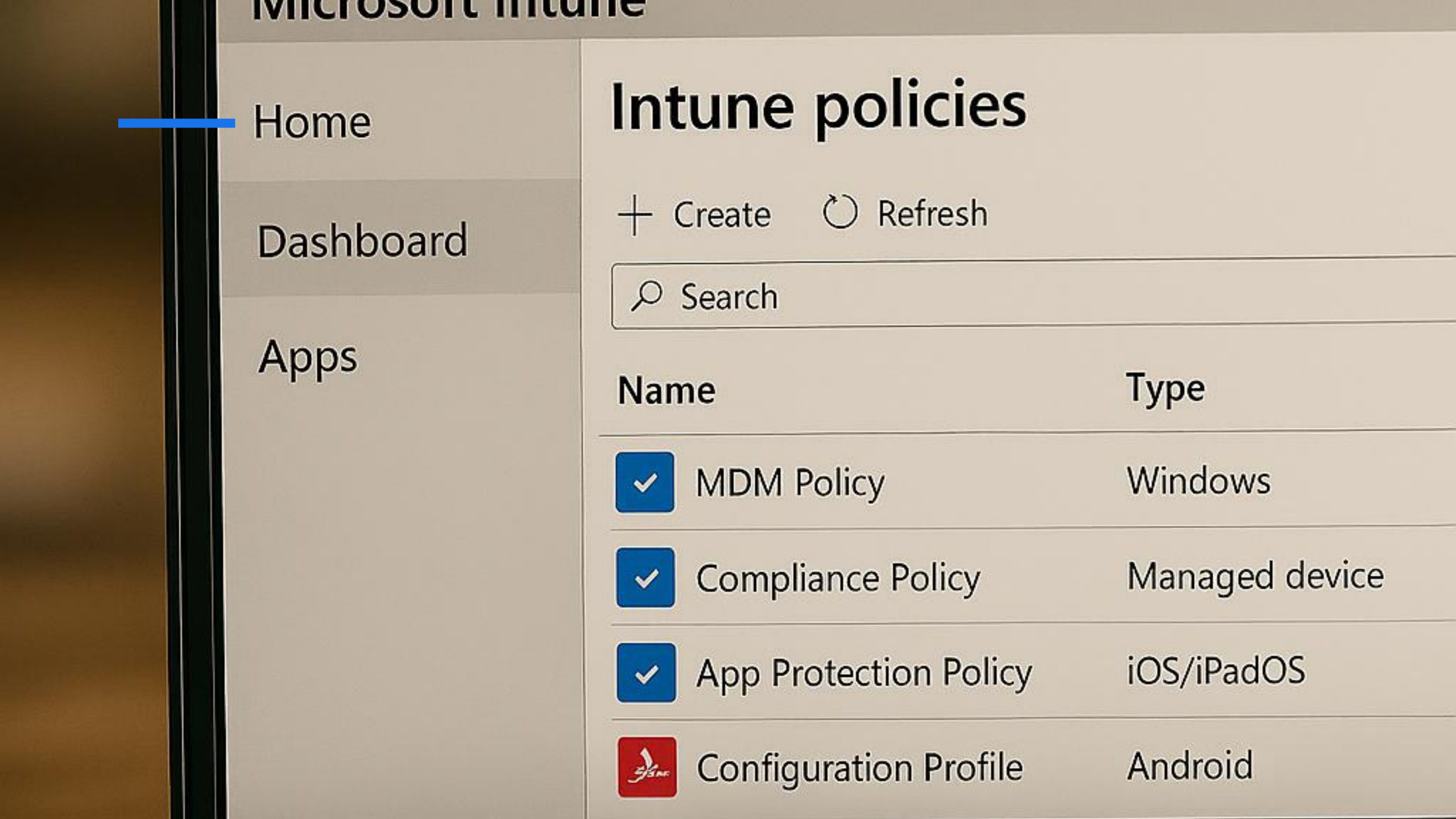
Script Deployment (Win32) - Autopilotbranding

The script is designed to be packaged into an Intune Win32 app. It supports a wide range of features including:

- Start menu and taskbar layout customization
- Background and lock screen configuration
- Removal of provisioned apps and optional features
- Installation of OneDrive and Edge for Business
- Language pack and feature-on-demand management
- Registry tweaks for branding and user experience

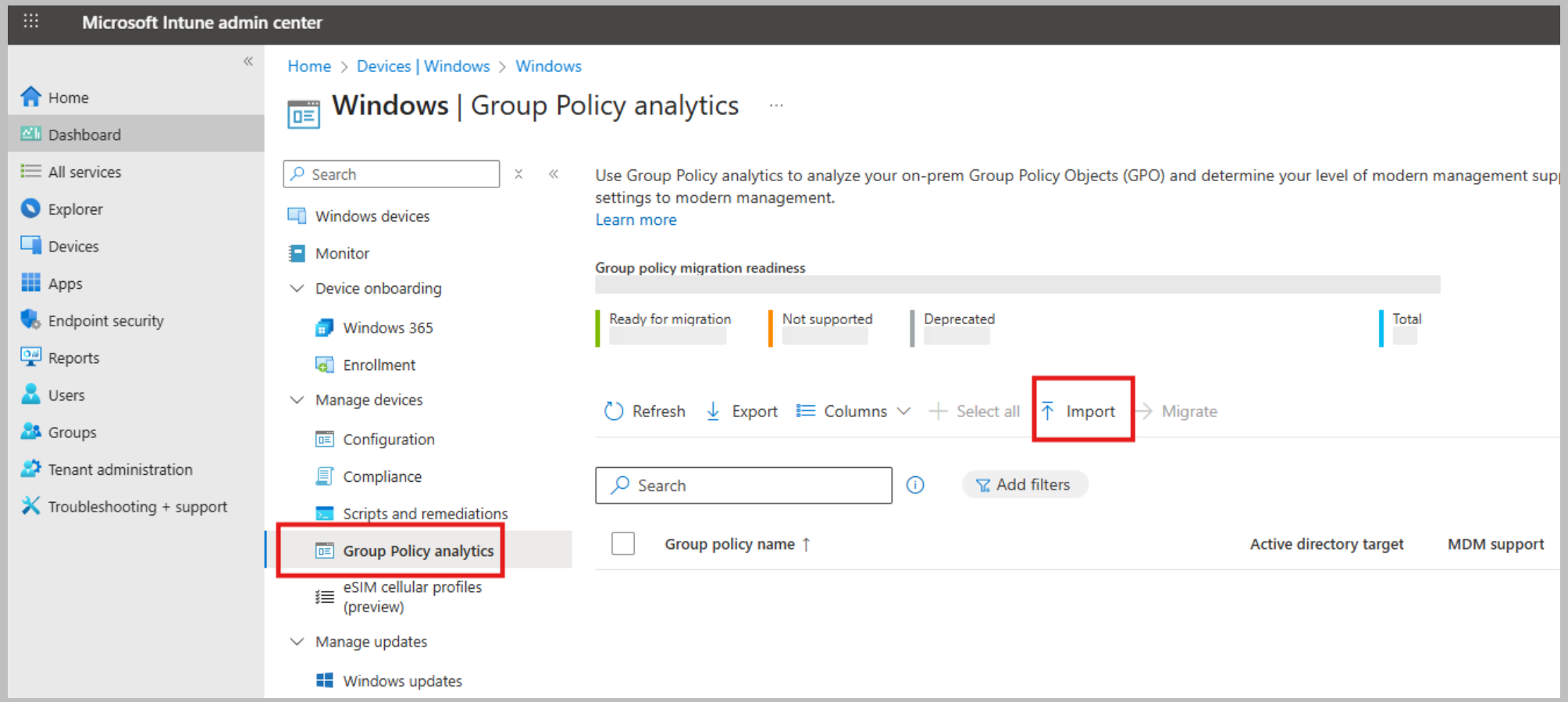
Troubleshoot – app deployment

1. Install the app locally via command line
2. Ensure the detection rule is valid, double check on your install command
3. Use MSI default switch - msiexec.exe /i "C:\Example.msi" /L*V "C:\package.log" then check the log
4. Some non-MSI installer has a log output switch too
5. Output logs from scripts you deployed as Win32 apps
6. You can find the log file even if the device fails during Autopilot
7. Contact app vendor who developed the app
8. CMTrace C:\ProgramData\Microsoft\IntuneManagementExtension\Logs


Microsoft Intune
Home
Dashboard
Apps
Intune policies
Create
Refresh
Search
Name
Type
MDM Policy
Windows
Compliance Policy
Managed device
App Protection Policy
iOS/iPadOS
Configuration Profile
Android

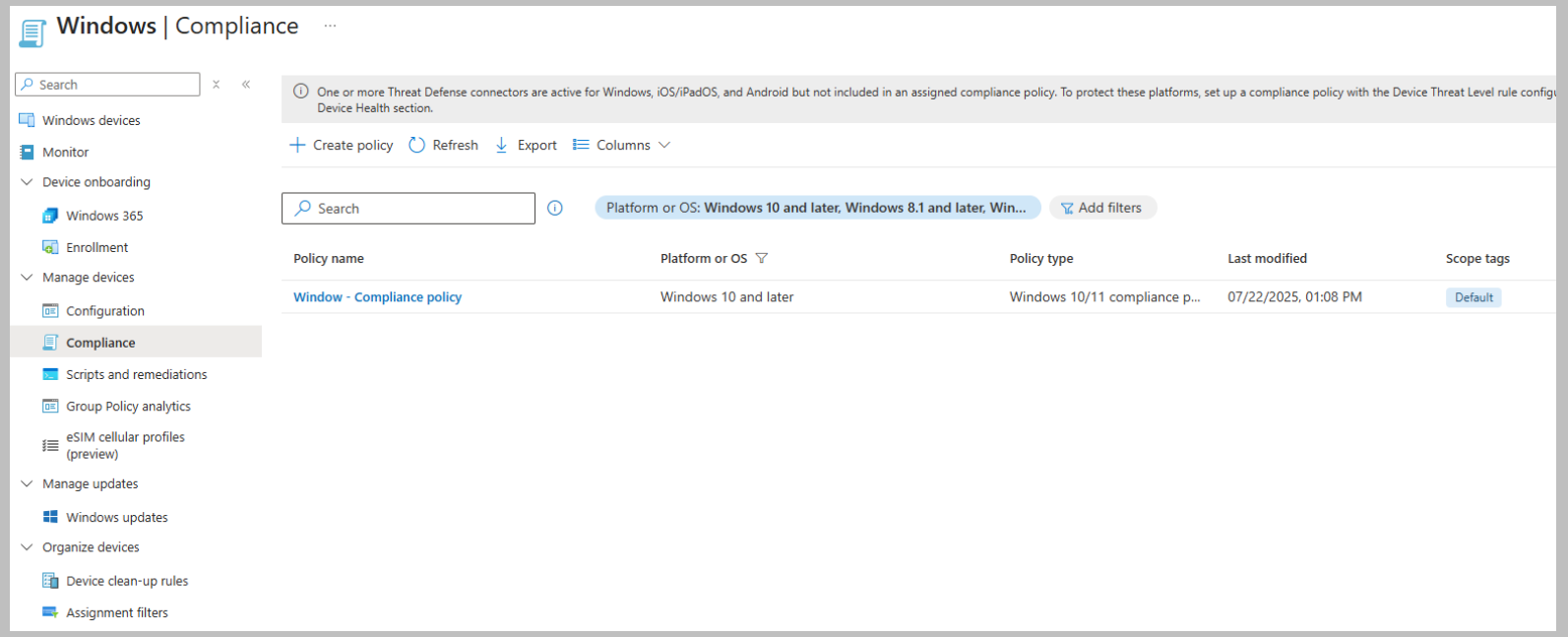
Group Policy Analytics

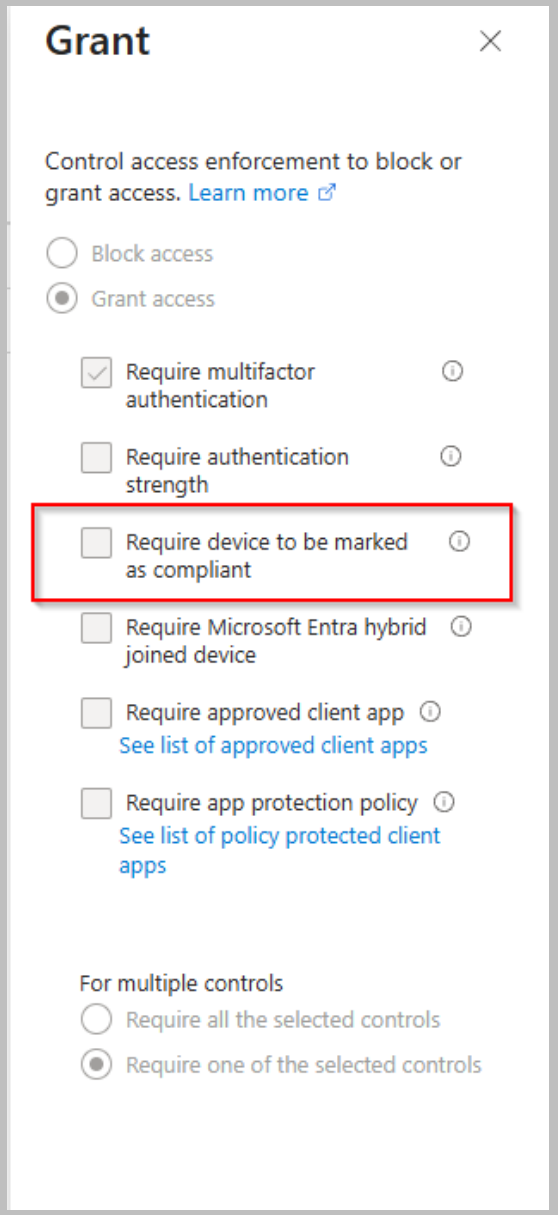
Group Policy Analytics in Microsoft Intune is a tool that helps organizations assess their existing on-premises Group Policy Objects (GPOs) and determine which settings can be migrated to Intune for cloud-based management



Compliance Policy

A **compliance policy in Intune** is a set of rules and conditions that define whether a managed device meets your organization's security and configuration requirements.





Shared drive mapping & printer mapping

Before using shared drive from on-prem file server, ask questions -

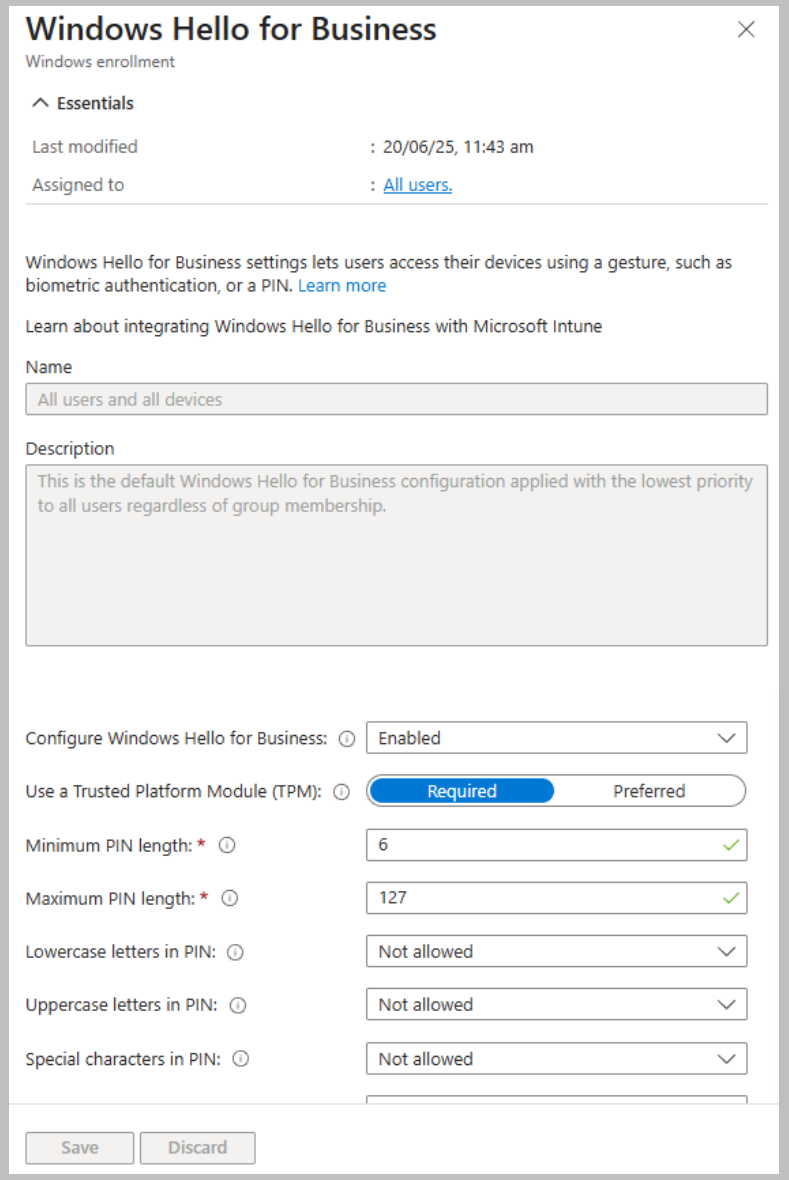
- Can we use Sharepoint online to replace shared drive?
- Can we use Teams or Azure files?
- Can we use Universal print?

https://intunedrivemapping.azurewebsites.net/

Windows Hello for Business

Windows Hello for Business (**WHfB**) is Microsoft's passwordless authentication method built into Windows 10 and Windows 11.

There is Intune policy you can deploy to specific devices.

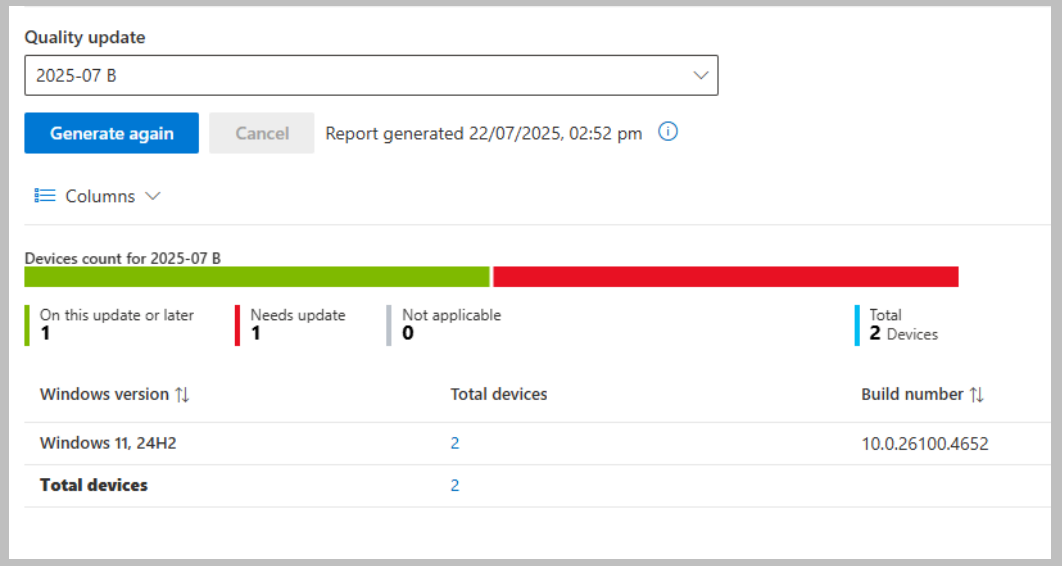


Windows Update for Business

Update ring settings Edit

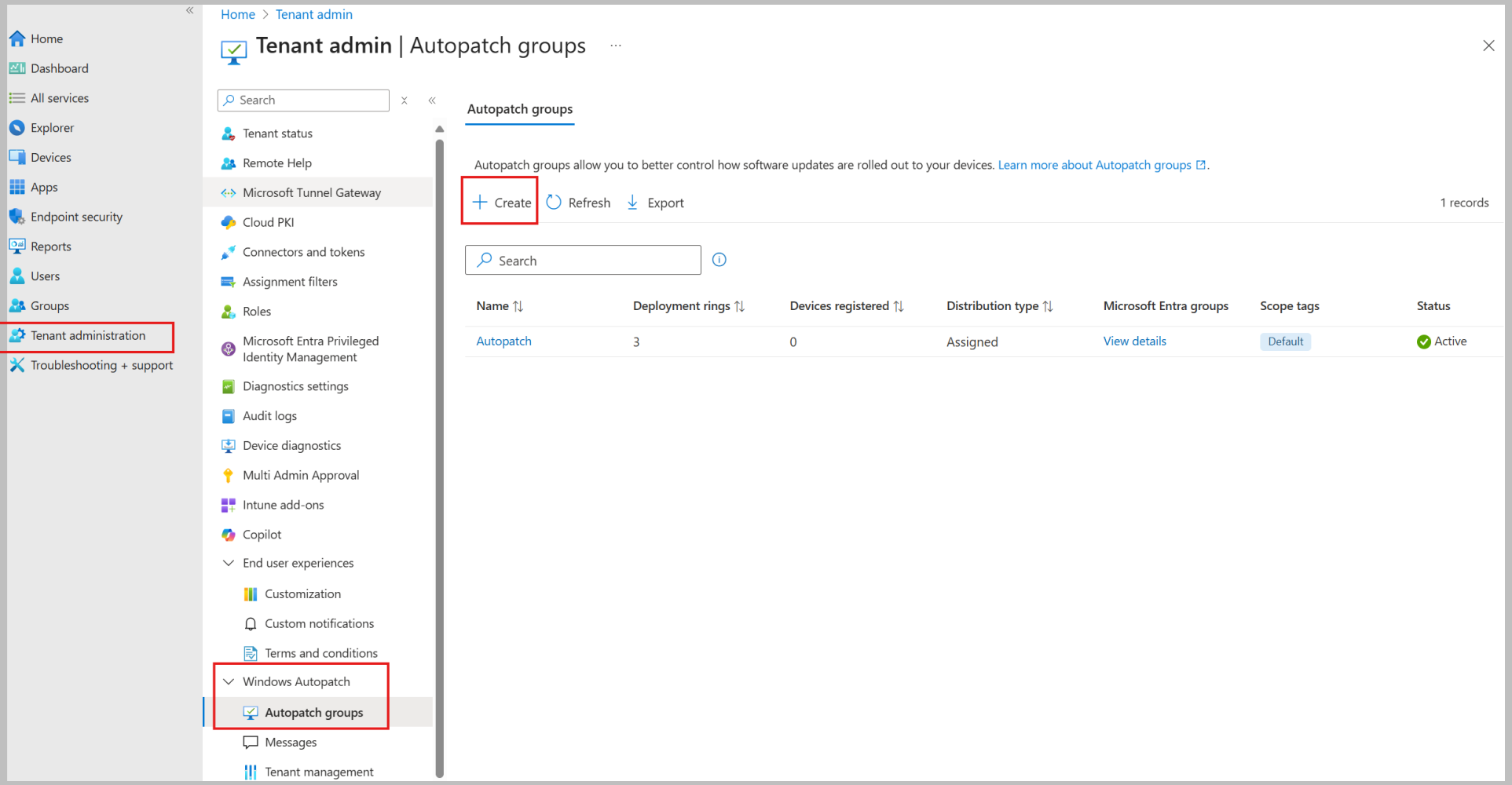
Update settings	
Microsoft product updates	Allow
Windows drivers	Allow
Quality update deferral period (days)	0
Feature update deferral period (days)	0
Upgrade Windows 10 devices to Latest Windows 11 release	No
Set feature update uninstall period (2 - 60 days)	10
Servicing channel	General Availability channel
User experience settings	
Automatic update behavior	Auto install at maintenance time
Active hours start	8 AM
Active hours end	5 PM
Option to pause Windows updates	Disable
Option to check for Windows updates	Enable
Change notification update level	Use the default Windows Update notifications
Use deadline settings	Allow
Deadline for feature updates	2
Deadline for quality updates	2
Grace period	7
Auto reboot before deadline	Yes

Reports are available in Intune portal, however some reports require E3 or E5 licenses to be generated



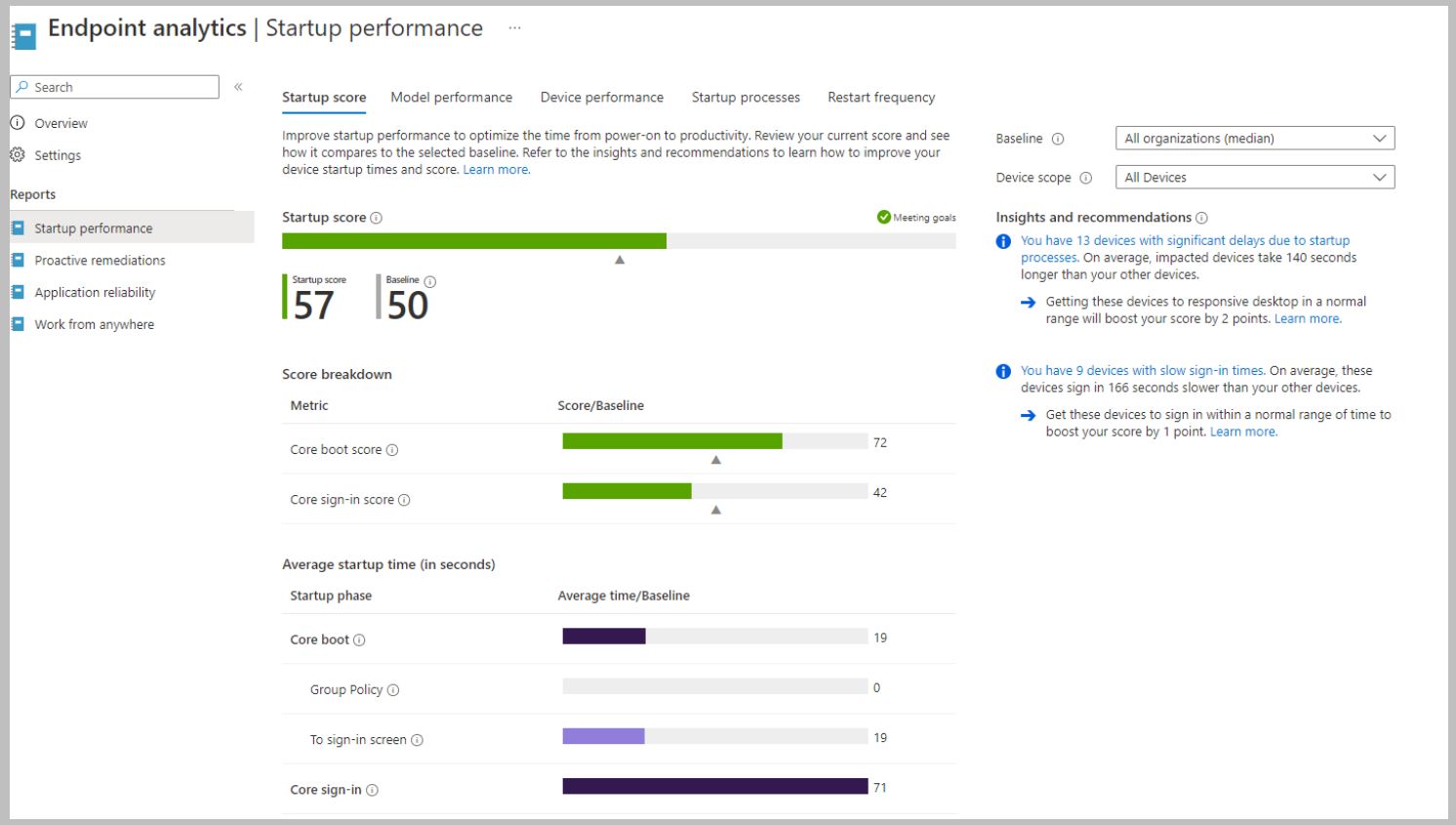
Autopatch

Autopatch is available with Business Premium license.
You can enable/deploy Autopatch by creating an Autopatch group



Endpoint Analytics

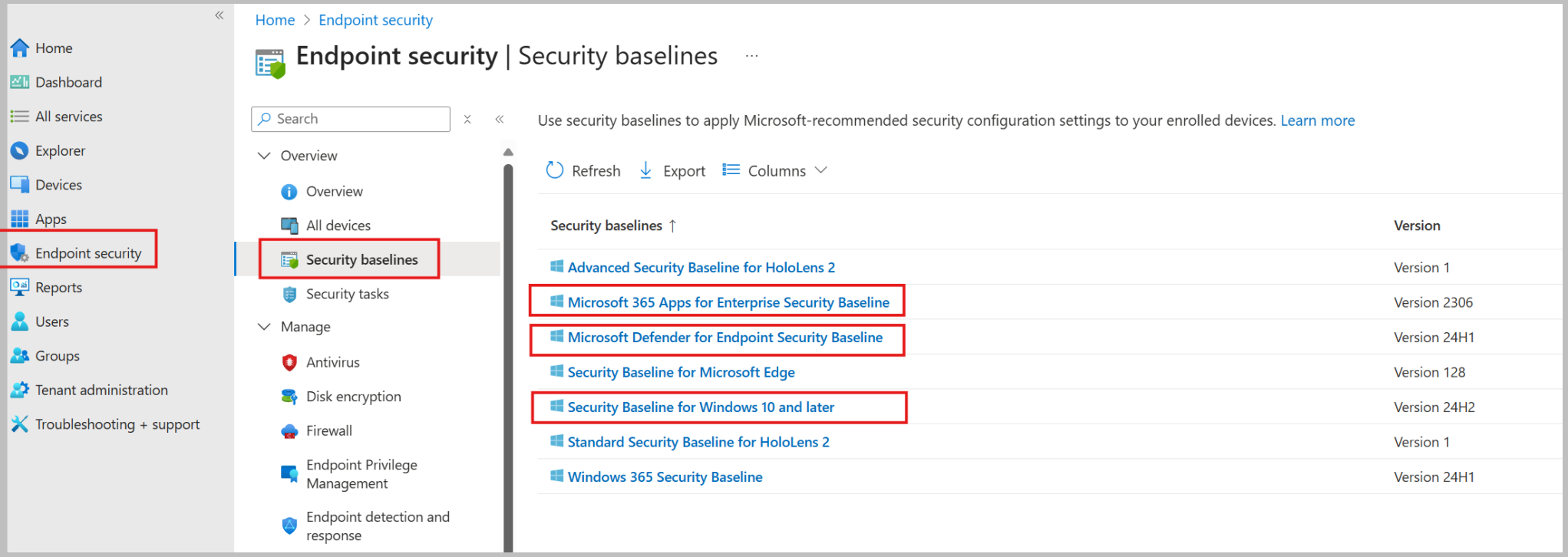
Endpoint analytics can help you to visualize the quality of the experience you're delivering to your users. Endpoint analytics can help identify policies or hardware issues that may be slowing down devices and help you proactively make improvements.



Intune integrations and security

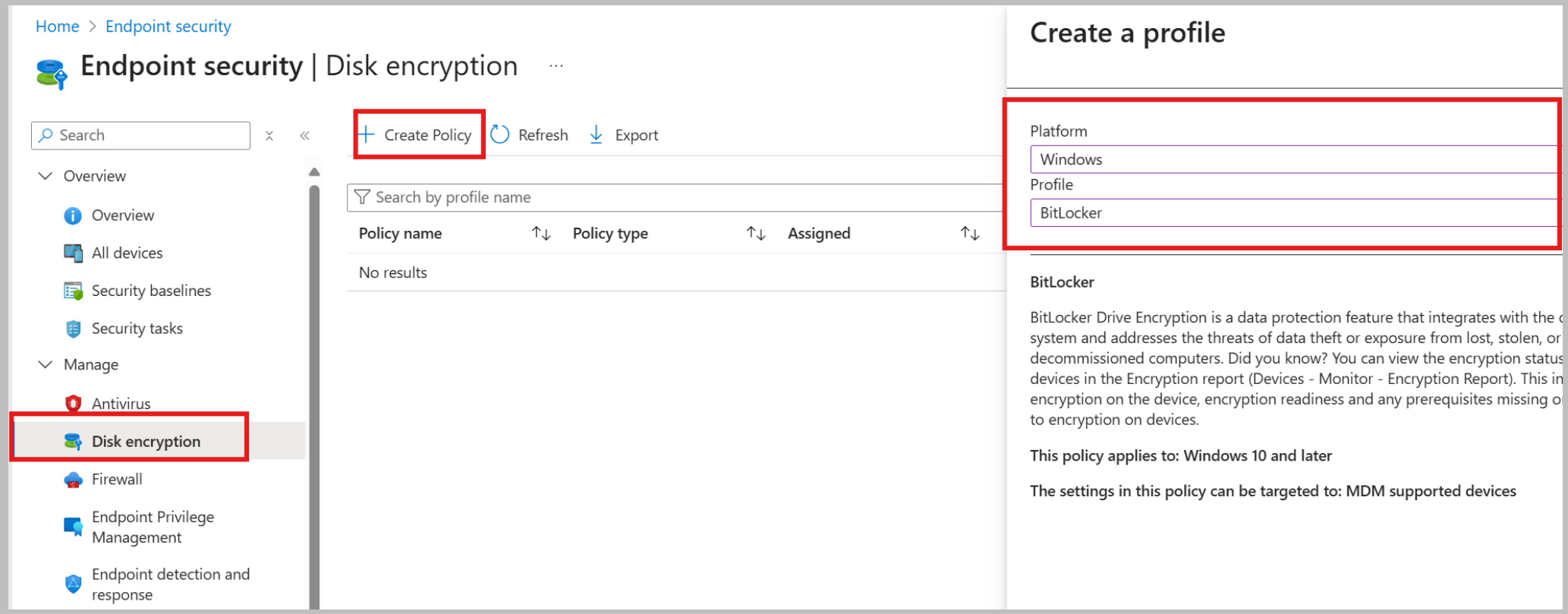
- Windows Autopilot for modern OS deployment and provisioning.
- Endpoint analytics for visibility and reporting on end user experiences, including device performance and reliability.
- Entra ID is used by Microsoft Intune for identity of devices, users, groups, multi-factor authentication (MFA) and many more.
- Microsoft Defender for Endpoint
- Microsoft Purview
- Microsoft Graph – every action in Intune can be achieved by Microsoft Graph API

Security baselines



- Do not deploy those templates until you know what they do. It is a good practice to separate one baseline into several different policies.
- Be aware of conflictions
- Does not necessary apply to Essential 8 – you can however modify accordingly to achieve different Essential 8 Maturity levels.

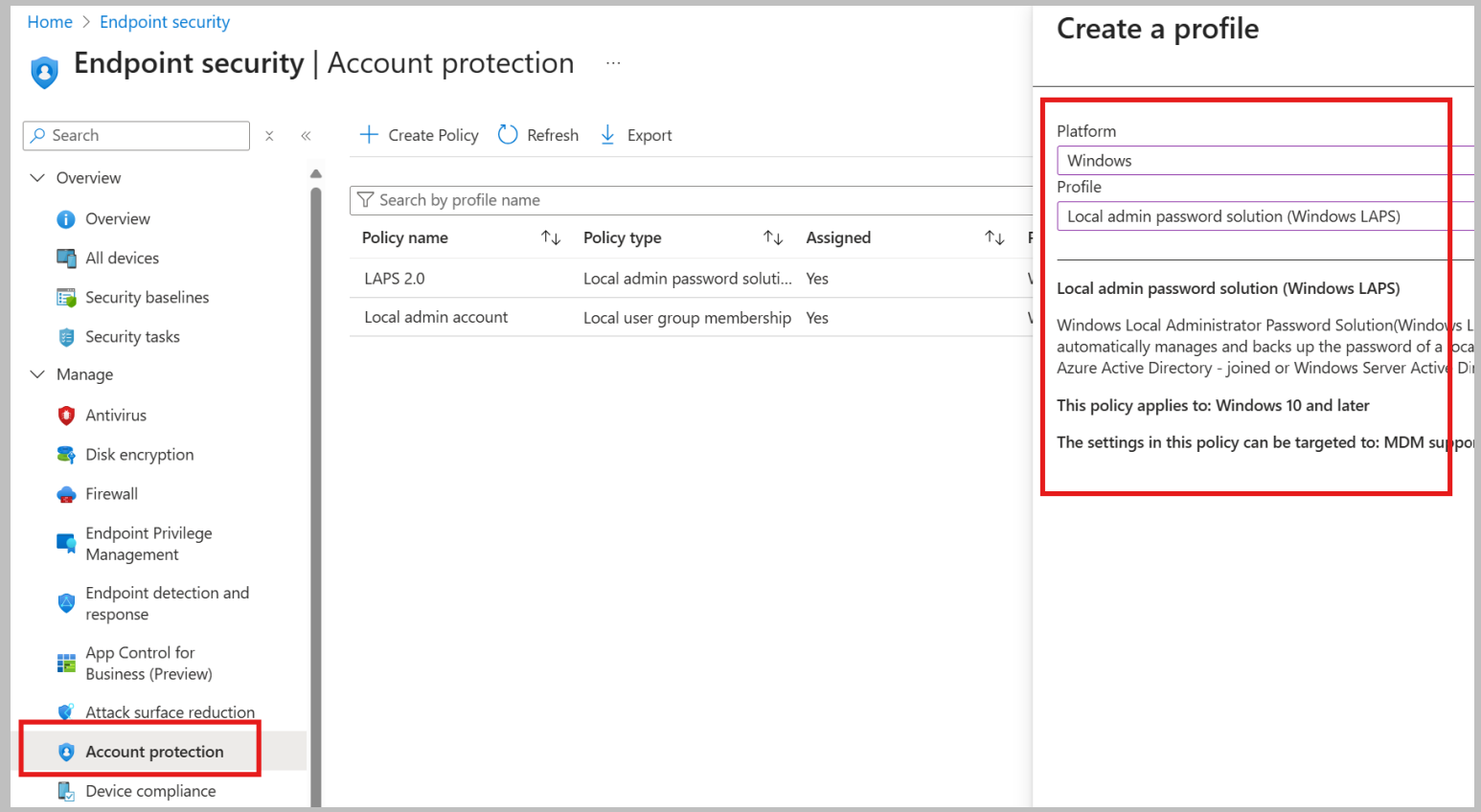
BitLocker



All Windows should have BitLocker enabled silently without user interaction.

https://learn.microsoft.com/en-us/intune/intune-service/protect/encrypt-devices

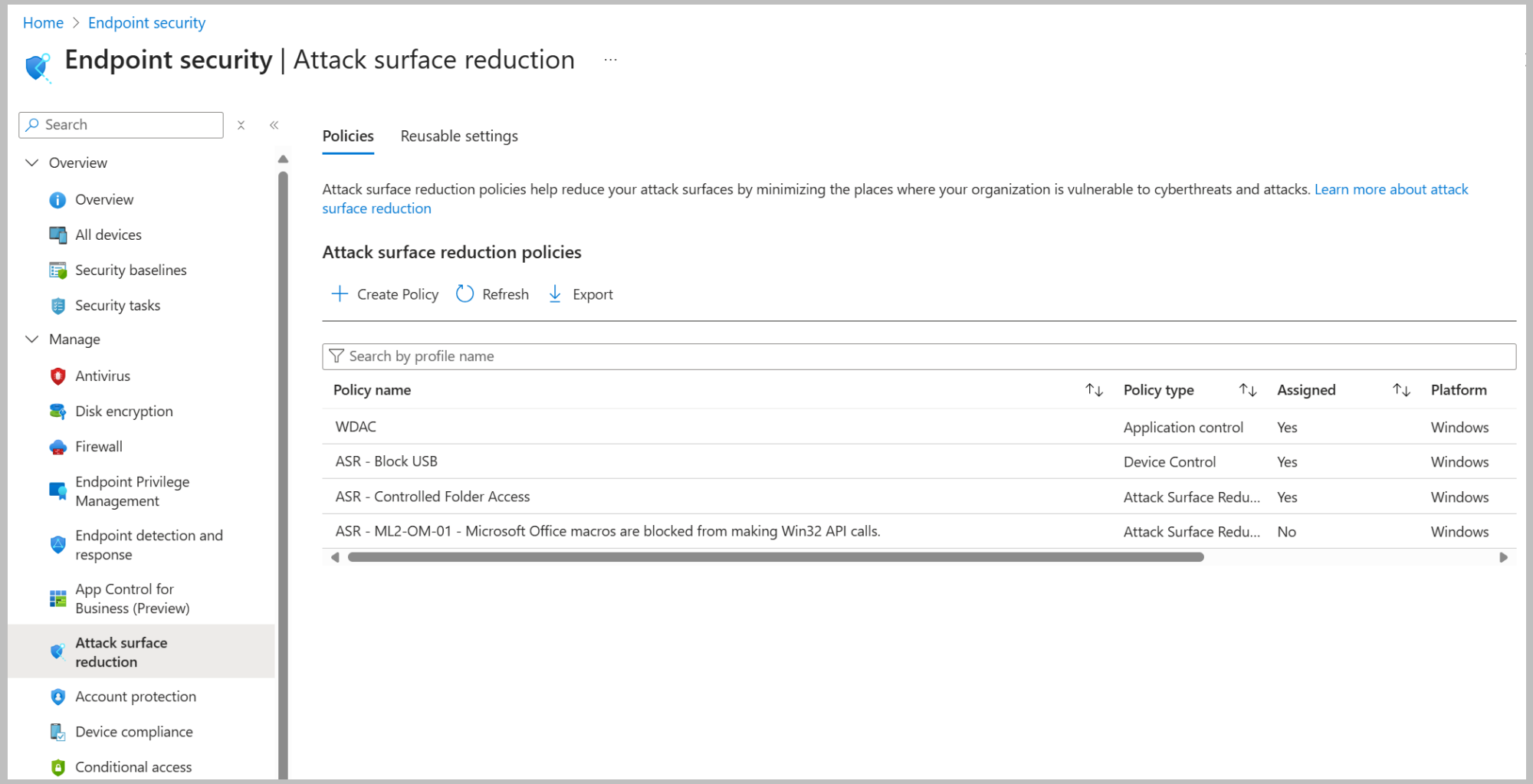
Local Admin Password Solution



Note that LAPS does not create a local account and LAPS can only manage one admin account per device.

https://learn.microsoft.com/en-us/intune/intune-service/protect/windows-laps-overview

Attack Surface Reduction

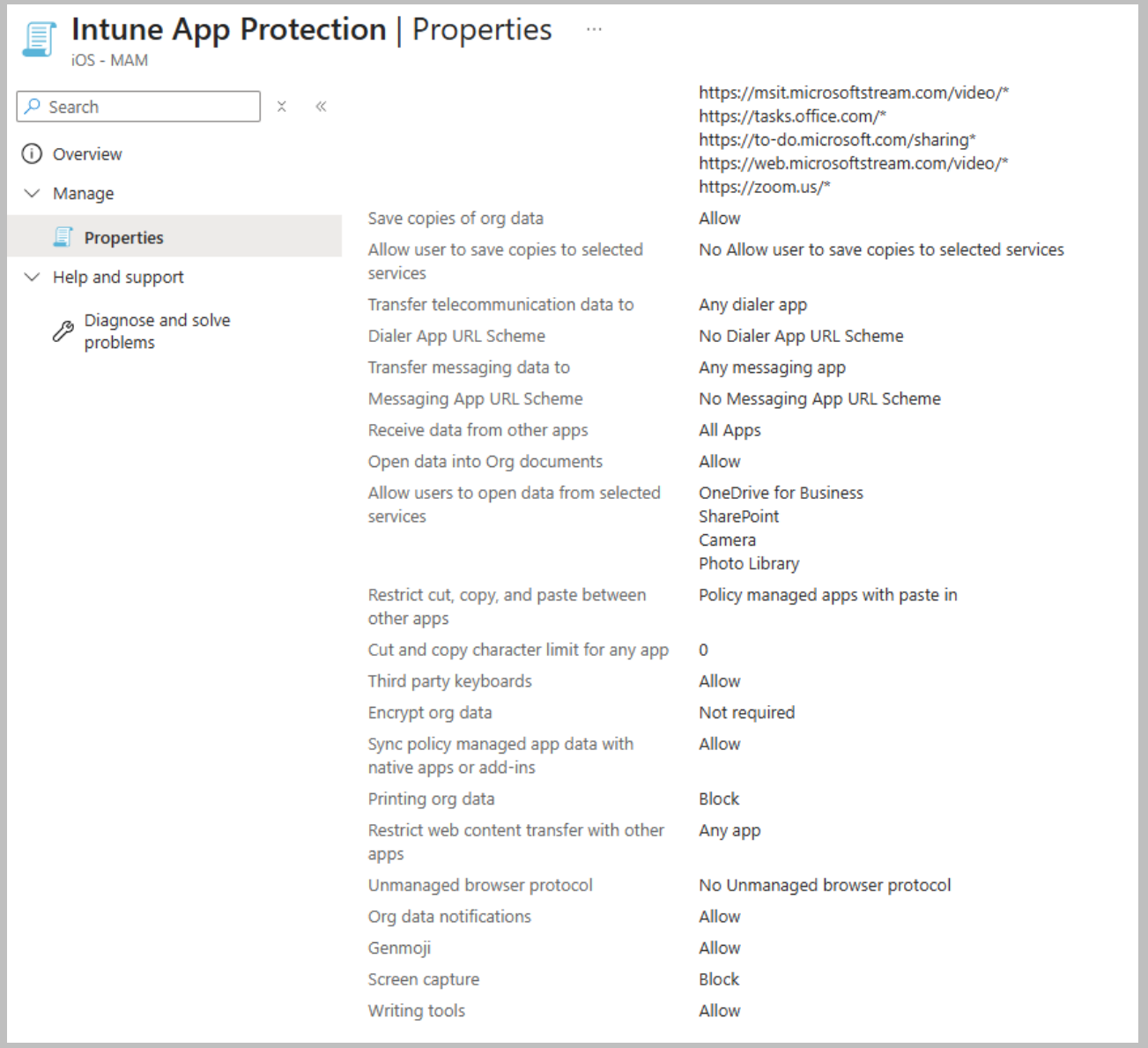


App protection - MAM

Typical Use Cases

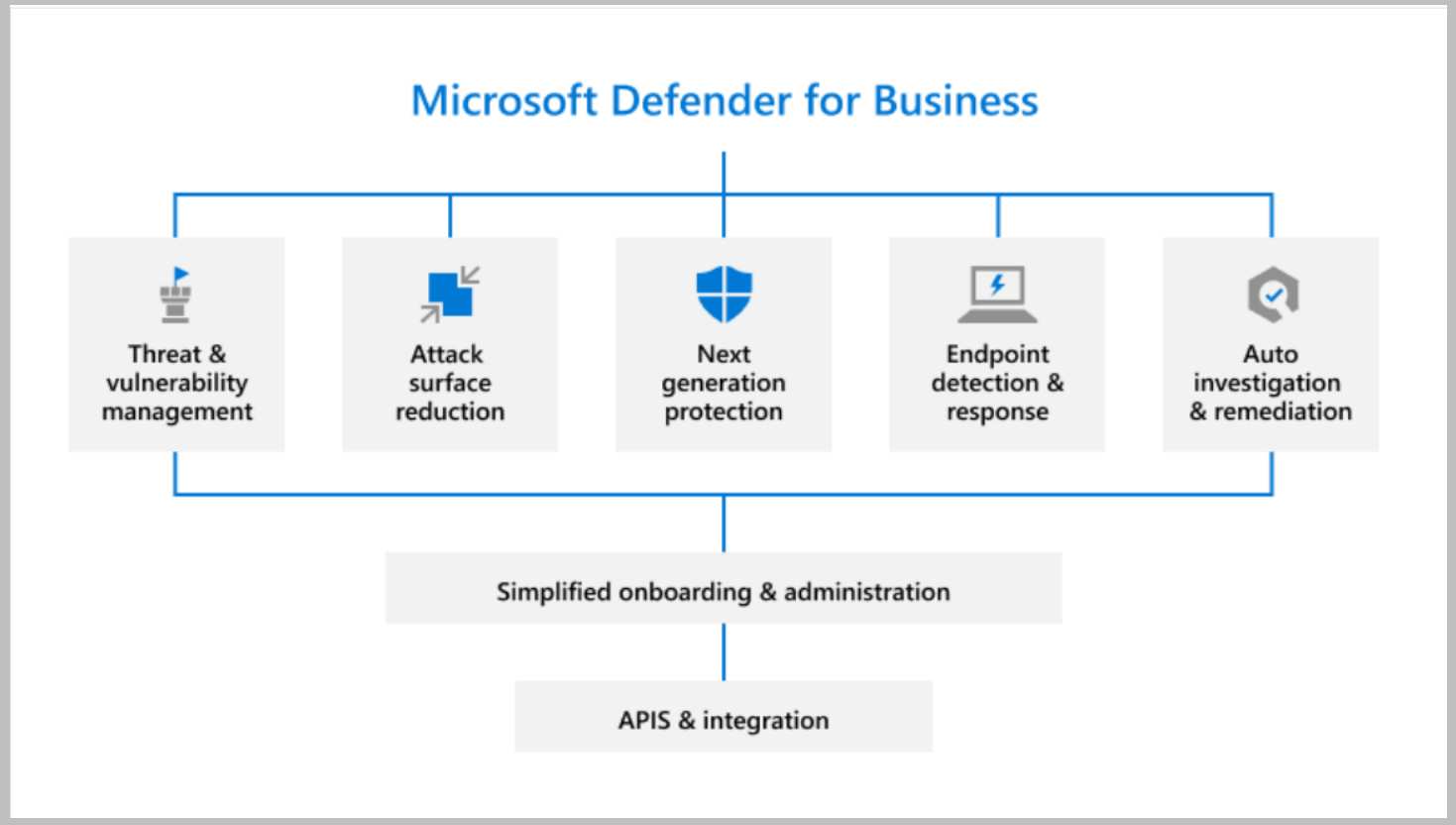
BYOD devices where users don’t want full device enrollment.

Frontline workers using shared devices but need app-level controls.



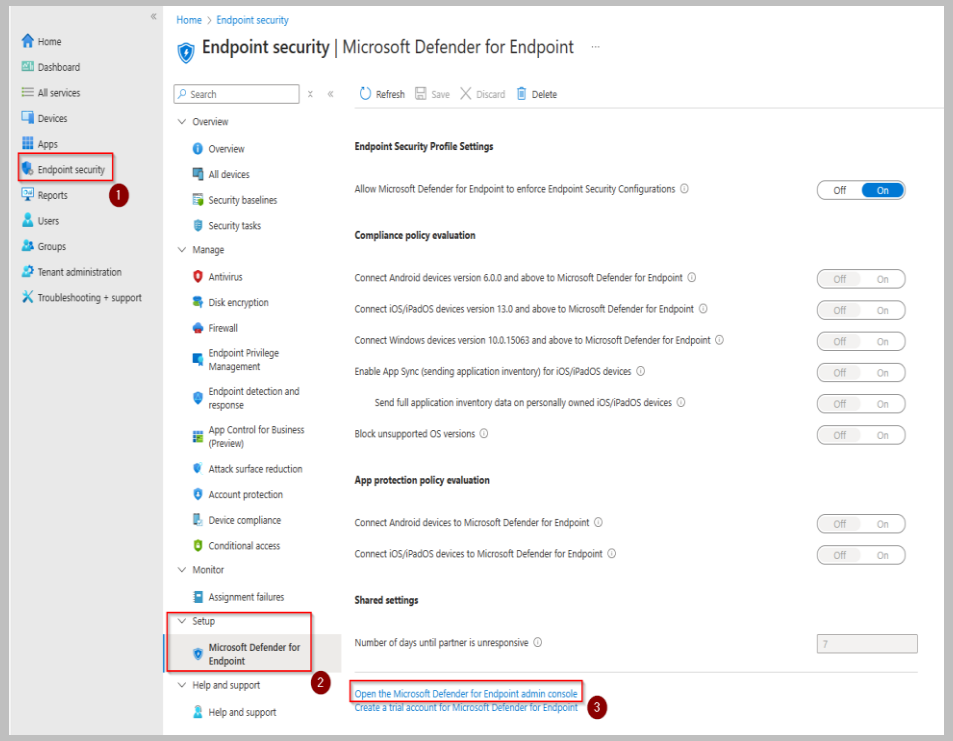
Microsoft Defender for Endpoint

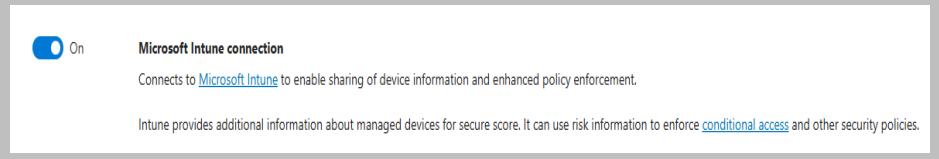
Microsoft Defender for Endpoint is a cloud platform integrated with Microsoft eco-system that manages endpoint security.



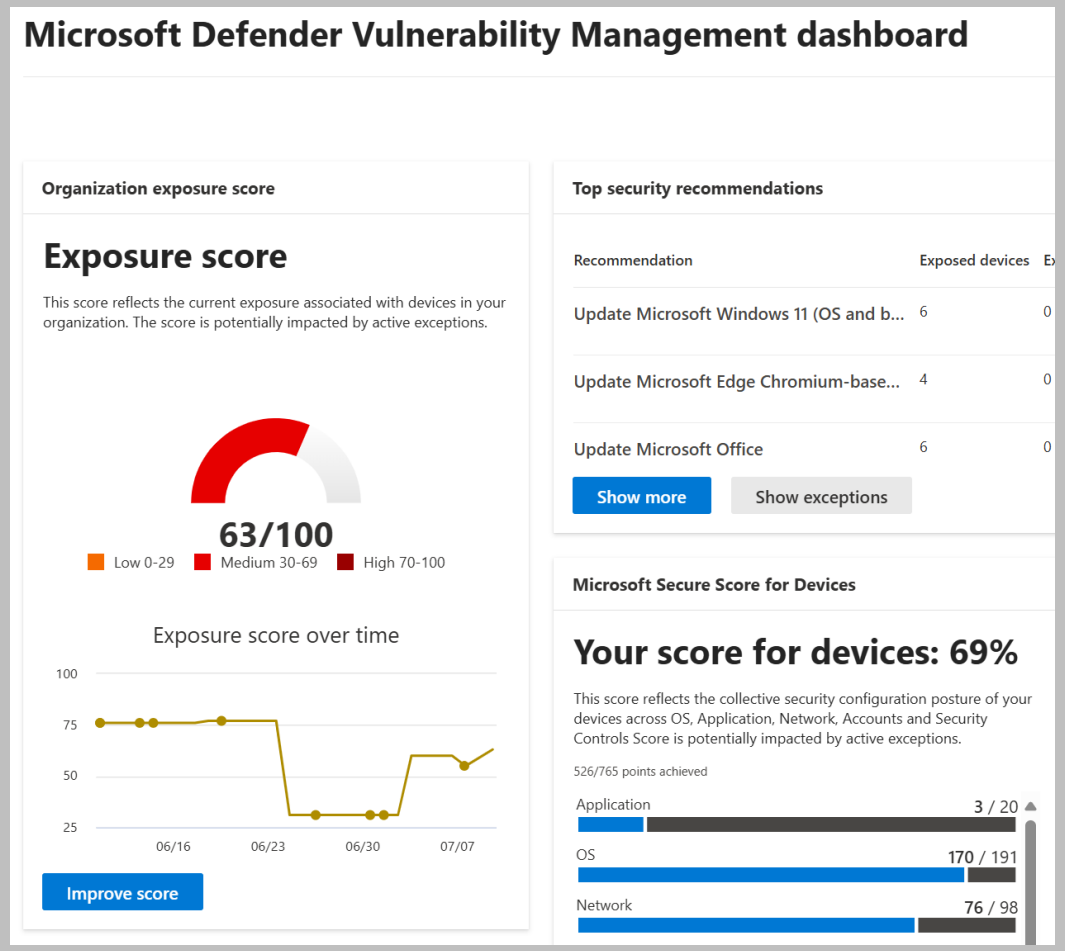
Onboarding

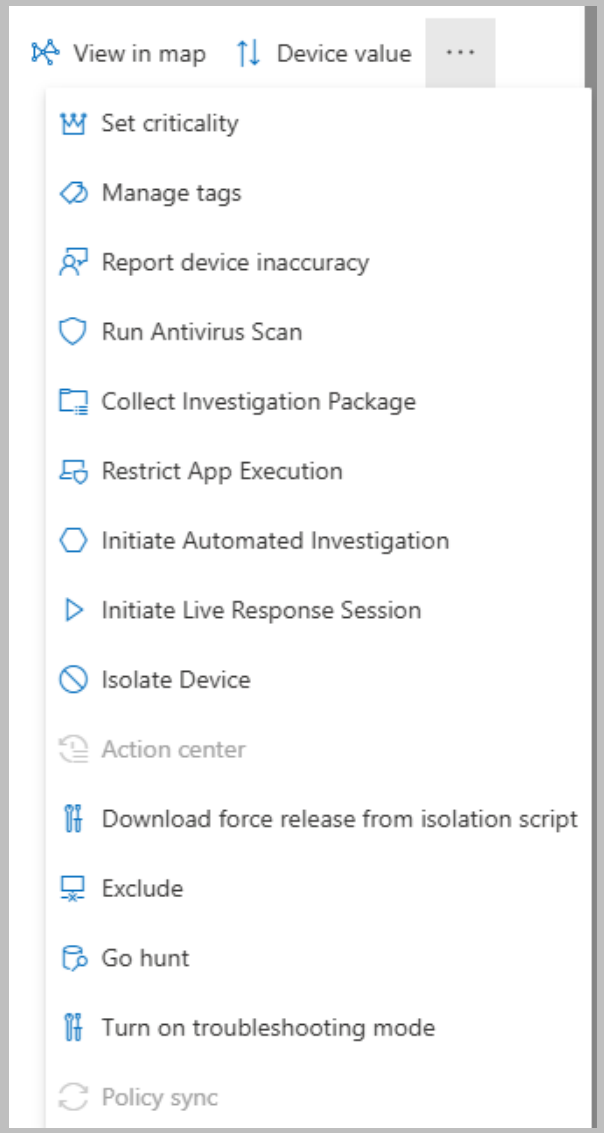
- Sign in to Intune portal
- Go to Endpoint security -> Microsoft Defender for Endpoint -> Open Microsoft Defender for endpoint admin console.
- Navigate to Settings -> Endpoints -> Microsoft Intune connection
- Go back to Intune portal and create a configuration profile -> Microsoft Defender for Endpoint -> assign to all devices





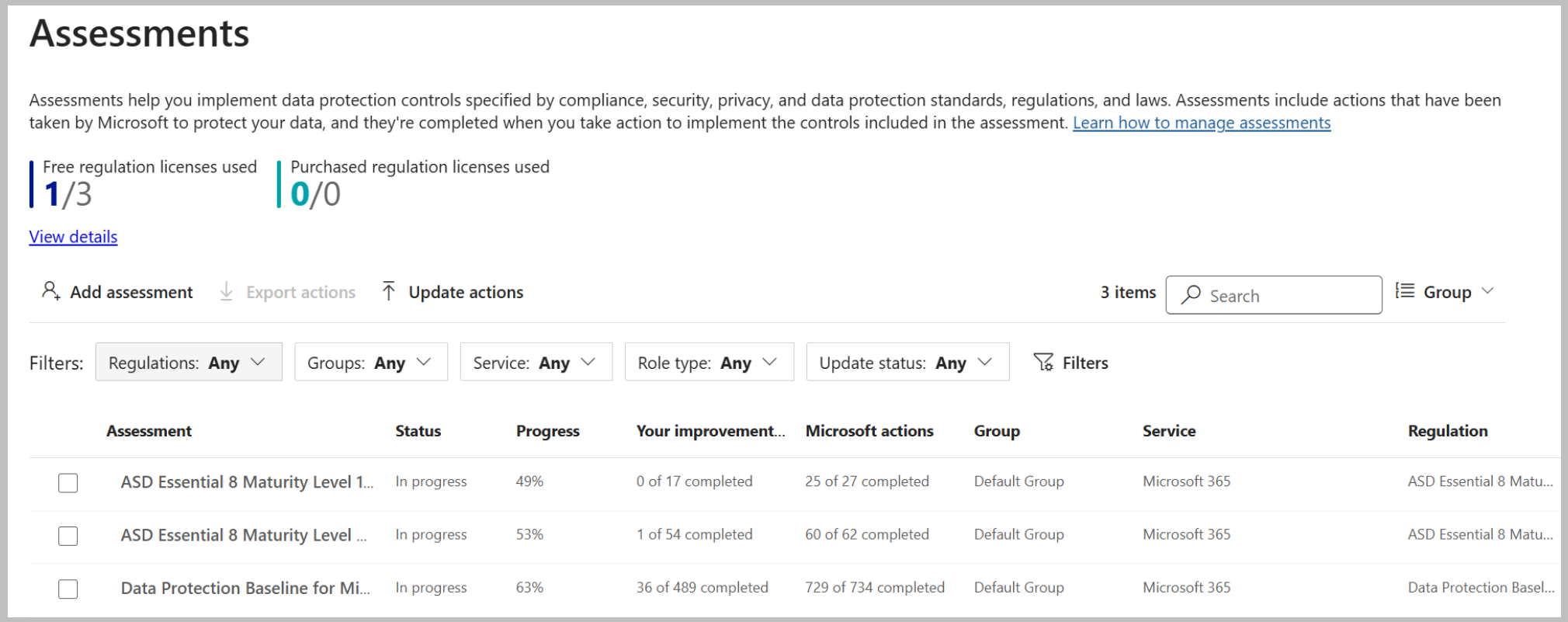
Vulnerability Management and Device Inventory





Compliance Manager

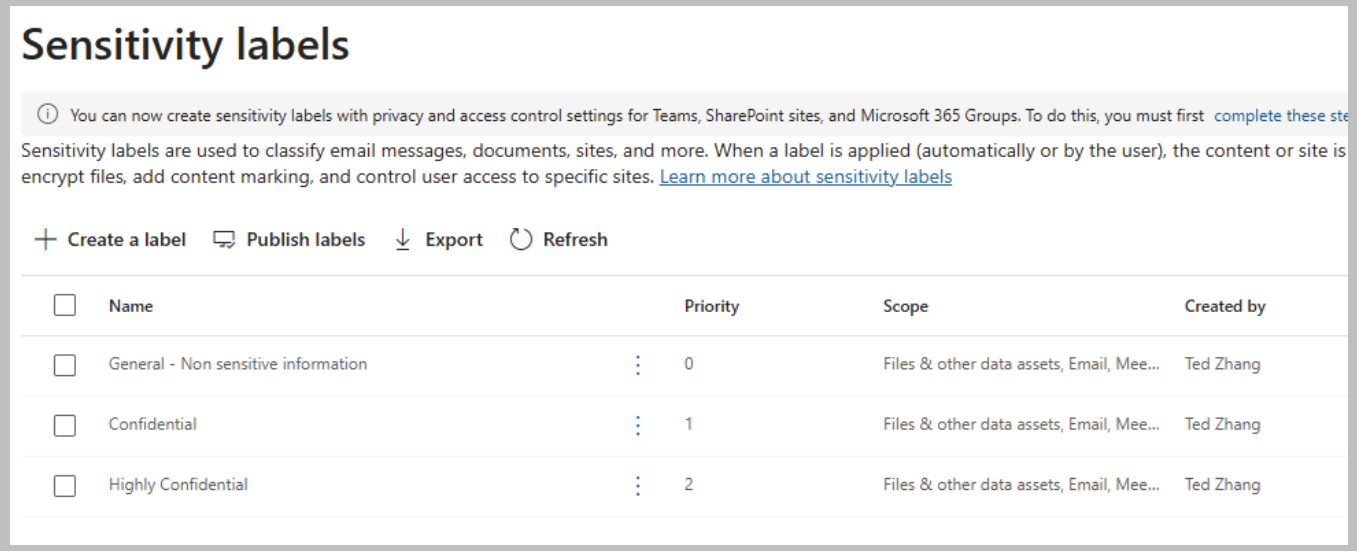
Microsoft Purview Compliance Manager is a solution that helps you automatically assess and manage compliance across your environment. Compliance Manager can help you staying current with regulations and reporting to auditors.

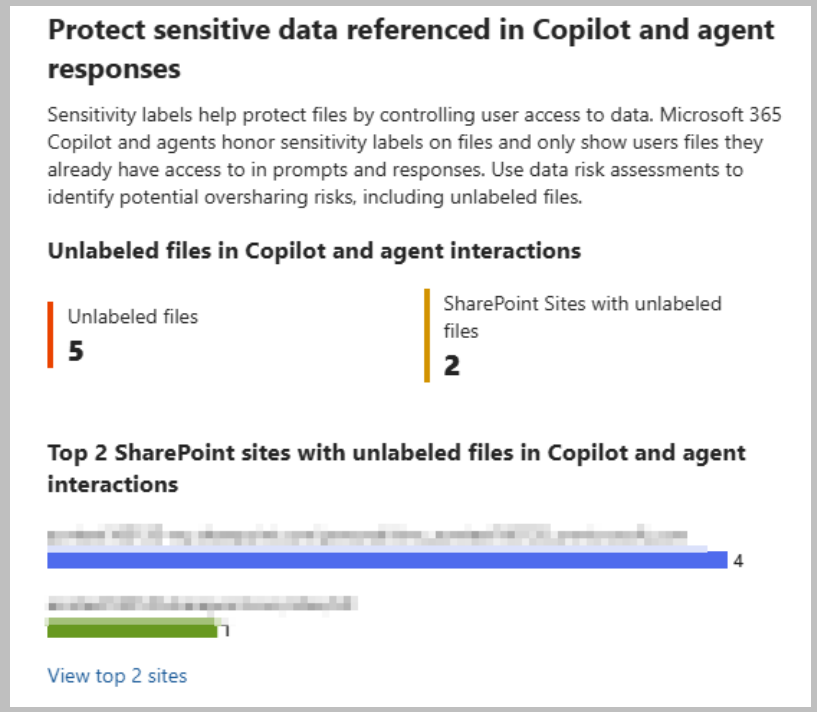


Sensitivity Label

When you assign a sensitivity label to content, it's like a stamp that's applied. It is customizable and persistent.

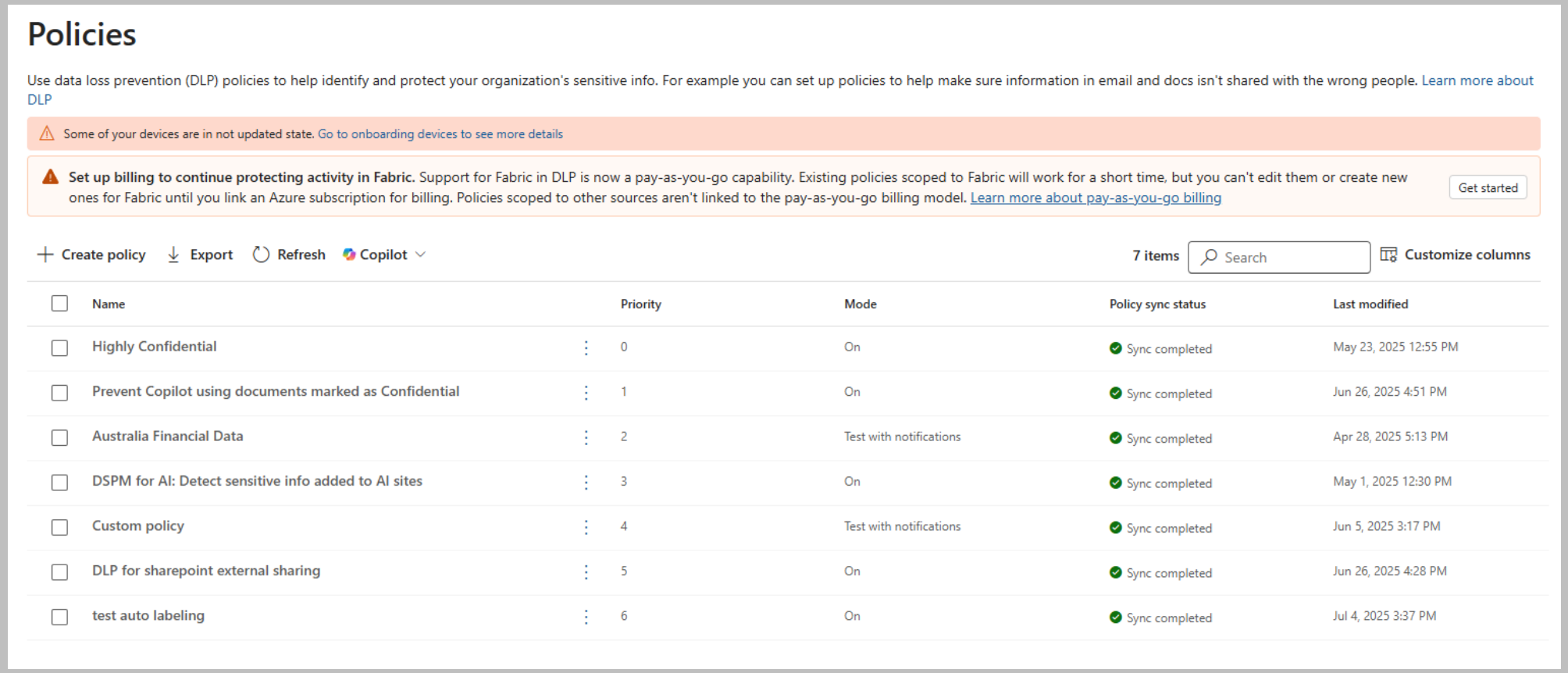
When viewed by users in your organization, an applied sensitivity label appears like a tag on apps and can be easily integrated into their existing workflows.





Data Loss Prevention (DLP)

Microsoft Purview Data Loss Prevention (DLP) helps you detect and prevent the unintentional sharing, transfer, or use of sensitive information across your Microsoft 365 environment.



What's my starting point?

- Secure score from Microsoft
- Adhere to a security framework – Essential 8, NIST, CIS, etc.
- Certifications

SALES SUPPORT

csp@au.synnex-grp.com

TECHNICAL SUPPORT

cspsupport@au.synnex-grp.com

CSP Microsite

https://csp.synnex.com.au/