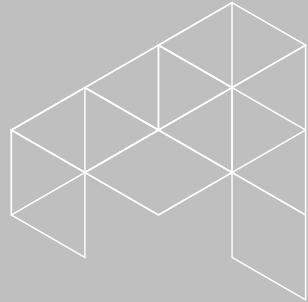
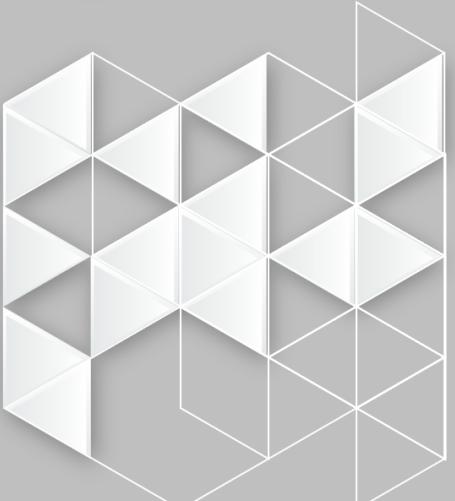




Microsoft Intune

Ted Zhang



Morning & Afternoon sessions

Morning Session

Introductions & Learning Pathways

Microsoft Intune & Autopilot

Intune Design fundamentals

Afternoon Session

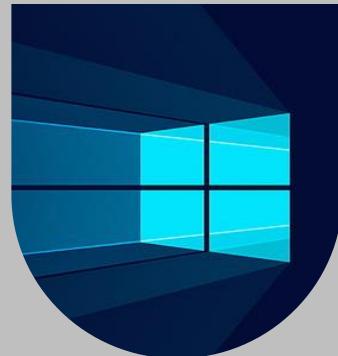
Intune Policy & Application Management

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.

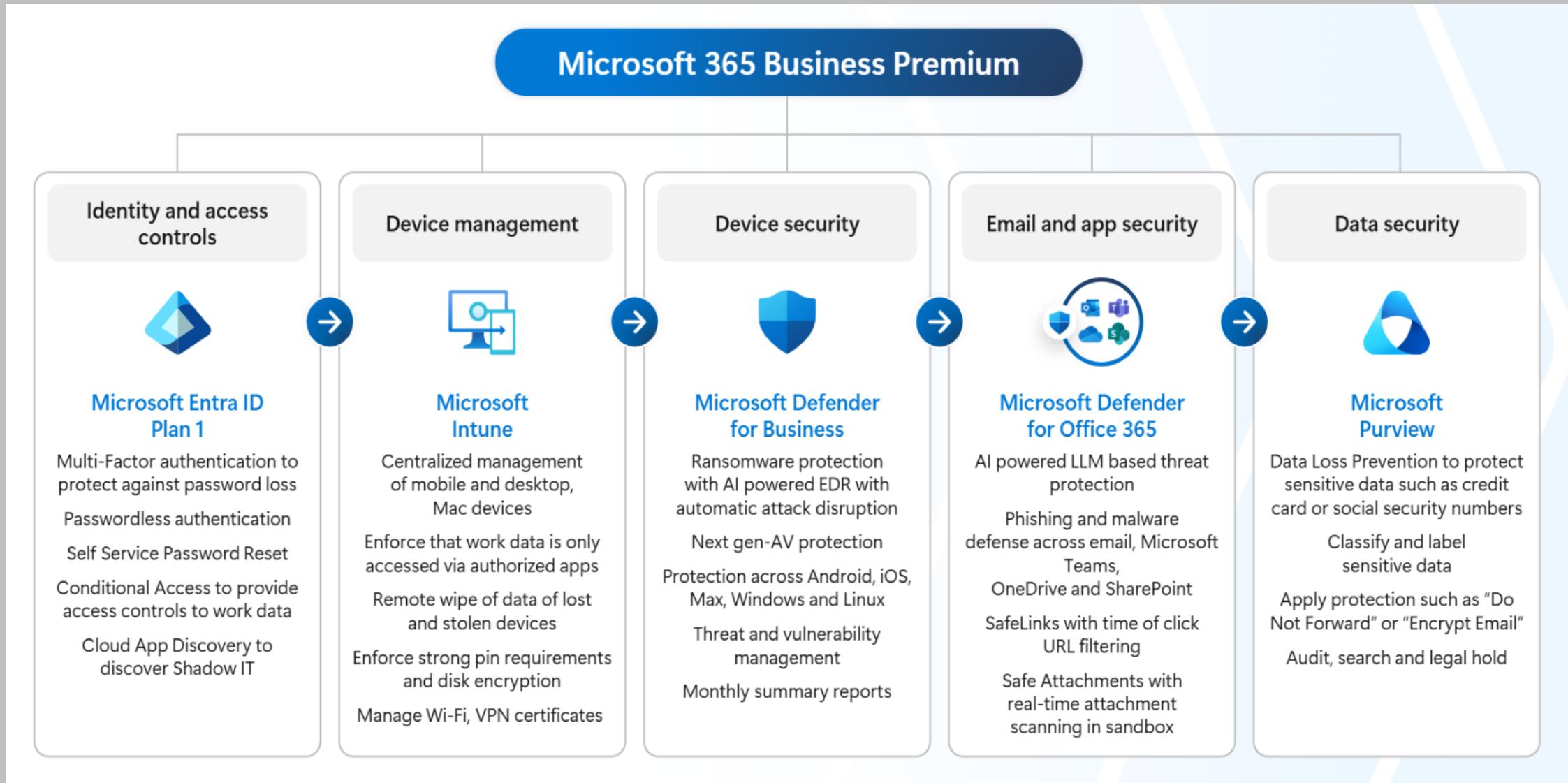
CIS controls and Essential 8

CIS Control	CIS Safeguard	Asset Class	Security Function	Title	Description	IG1	IG2	IG3
1				Inventory and Control of Enterprise Assets	<i>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.</i>			
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



Microsoft Incentives

\$4.4K Incentives earned when expanding from 100 seats to 200 seats of Business Premium through CSP



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)	<i>Innovate and Balance countries*</i> : 3.00%	\$75,000*
	<i>Scale countries**</i> : 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](#).

Category	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
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/>

Upskill Rewards Program

As part of our ongoing commitment to continuously empower and enable our partners, we've introduced the Upskill Rewards Program to incentivise partners to attain Microsoft certifications.

Partners that successfully pass eligible Microsoft certification exams during the program period can claim fixed subsidy amount from Synnex. Please refer to the [Terms and Conditions](#) document for full program details.

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

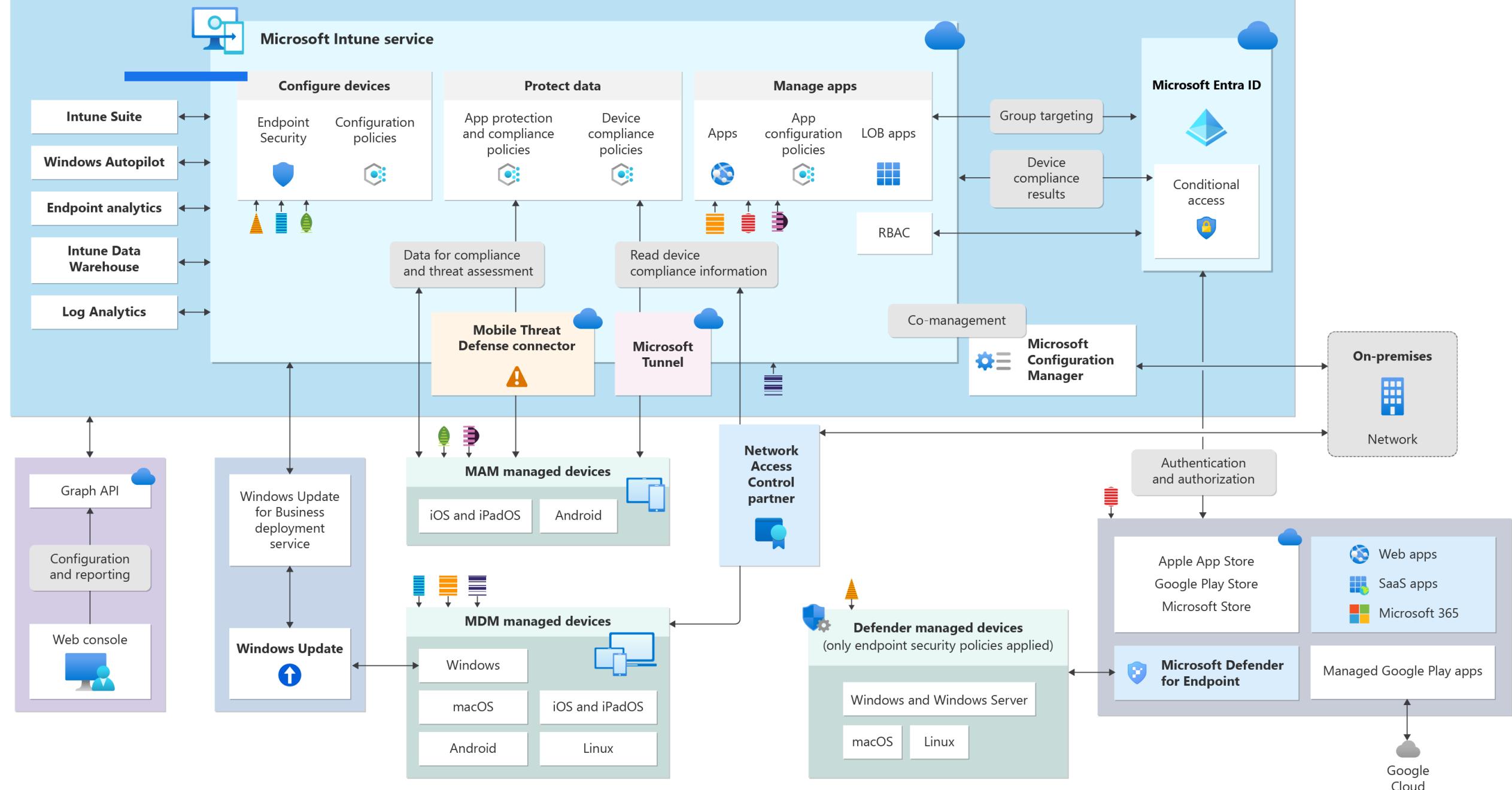
Overview of Microsoft Intune

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



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

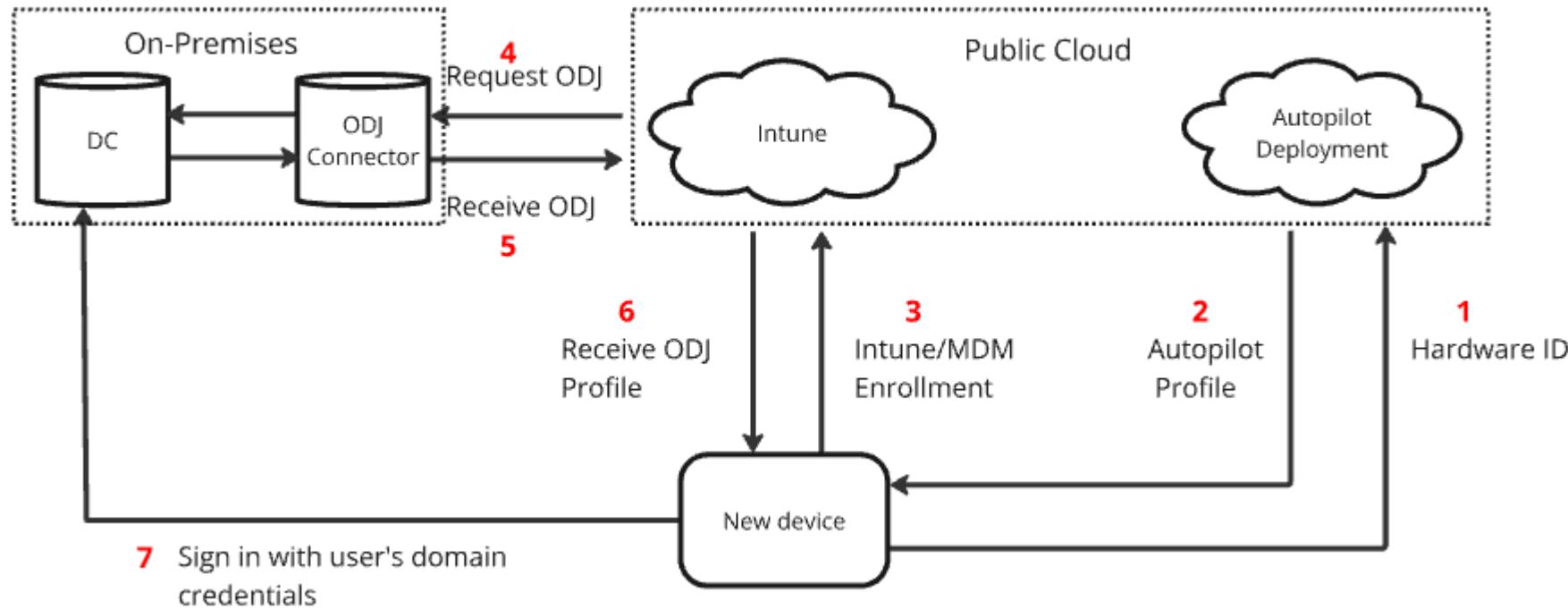


Hybrid Join Setup

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

Hybrid Join workflow (Simplified)

Hybrid Entra ID Join with Autopilot



Benefits of Hybrid Join

Access to On-Prem Resources

File shares, legacy apps, on-prem printers

Group Policy

Full GPO support

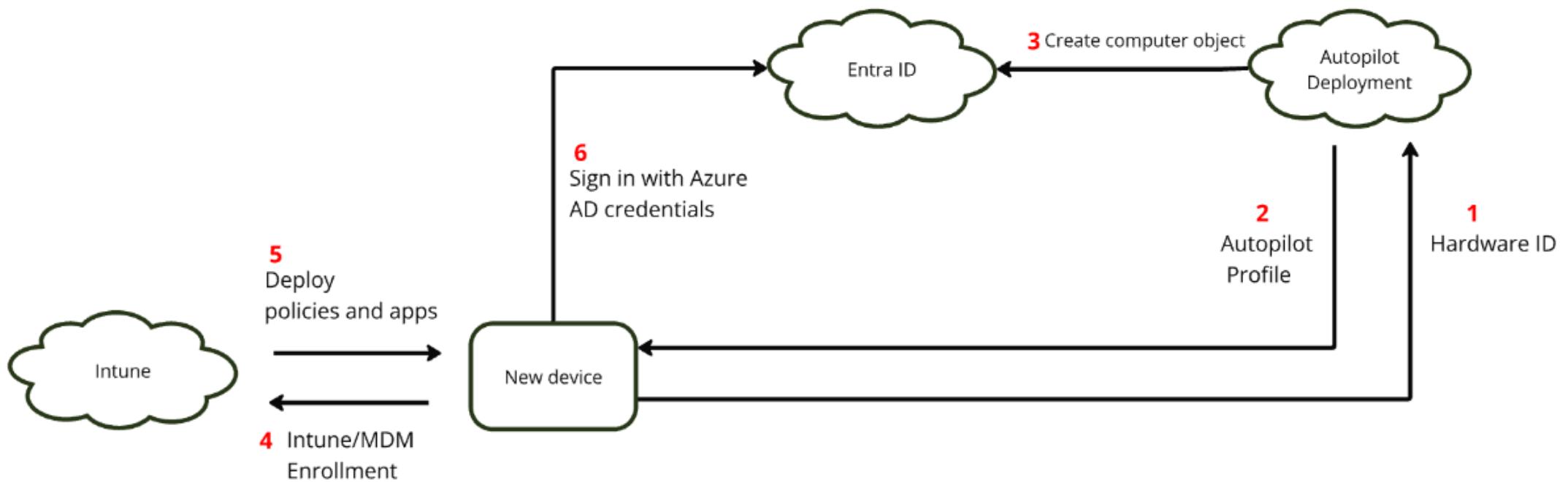
Certificate (via On-prem Certificate Authority)

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



Entra ID Join workflow

Entra ID Join with Autopilot



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 conflicts
- 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.

The screenshot shows the Microsoft Intune Device Overview page for a device named "HELLOP". The top navigation bar includes links for Home, Windows | Windows devices, and a search bar. Below the navigation is a toolbar with actions: Retire, Wipe (highlighted with a red box), Delete, Remote lock, Sync, Reset passcode, Restart, Fresh Start, Autopilot Reset, Quick scan, and Full scan. On the left, a sidebar menu lists Overview, Manage (Properties, Monitor, Resource explorer, Hardware, Discovered apps, Device compliance, Device configuration, App configuration, Recovery keys, User experience), and a collapsed section for Device actions status. The main content area displays device details under the "Essentials" tab. The "Ownership" field is highlighted with a red box. Other fields include Device name (HELLOP), Management name (testted_Windows_8/7/2025_1:28 AM), Serial number (0F00JC623233BF), Phone number (---), Device manufacturer (Microsoft Corporation), Primary user (test ted), Enrolled by (test ted), Compliance (Compliant), Operating system (Windows), Device model (Surface Pro 9), Last check-in time (8/7/2025, 11:34:14 AM), and Remote assistance (Not configured). The bottom section shows the "Device actions status" table with columns for Action, Status, Date/Time, and Error, and a single entry: No data.

Action	Status	Date/Time	Error
No data			

<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



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.

Device deployment details

3e65474b-5553-4faf-840c-8f31084bf32d

Device Apps Scripts

Refresh Columns ▾

Search Add filters

Review the app install status during deployment for the apps selected in the device preparation profile and dependency apps. [Learn more about app status during Autopilot device preparation.](#)

App name	Status	Selected	App type
Adobe Acrobat Reader DC	Skipped	Yes	WinGetSto...
AutopilotBranding	Skipped	Yes	WindowsCl...
Company Portal	Skipped	Yes	WinGetSto...

Device deployment details

3e65474b-5553-4faf-840c-8f31084bf32d

Device Apps Scripts

Refresh Columns ▾

Search Add filters

Review the PowerShell scripts install status during deployment for the scripts in the device preparation profile. [Learn more about script status during Autopilot device preparation.](#)

Script name	Status
timezone	Skipped
admin	Skipped
Modern Workplace - Autopatch C	Skipped

[Known issue: Windows Autopilot device preparation with Win32 apps and managed installer policy | Microsoft Community Hub](#)

Autopilot device preparation vs Autopilot

Supported modes	<ul style="list-style-type: none">User-driven.Automatic.	<ul style="list-style-type: none">User-driven.Pre-provisioned.Self-deploying.Existing devices.
Join types supported	<ul style="list-style-type: none">Microsoft Entra join.	<ul style="list-style-type: none">Microsoft Entra join.Microsoft Entra hybrid join.
Device registration required?	No.	Yes.
What do admins need to configure?	<ul style="list-style-type: none">Windows Autopilot device preparation policy.Device security group with Intune Provisioning Client as owner.	<ul style="list-style-type: none">Windows Autopilot deployment profile.Enrollment Status Page (ESP).
What configurations can be delivered during provisioning?	<ul style="list-style-type: none">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.	<ul style="list-style-type: none">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	

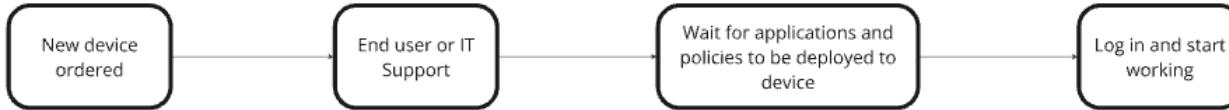
Autopilot with pre-provisioning/whiteglove

Autopilot Scenarios

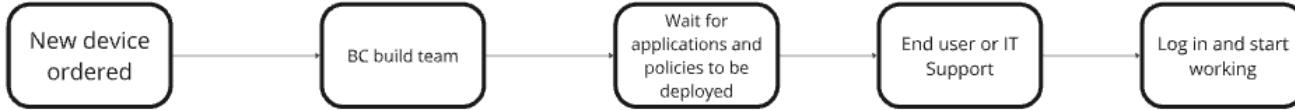
User Driven Deployment with Enrollment Status Page disabled



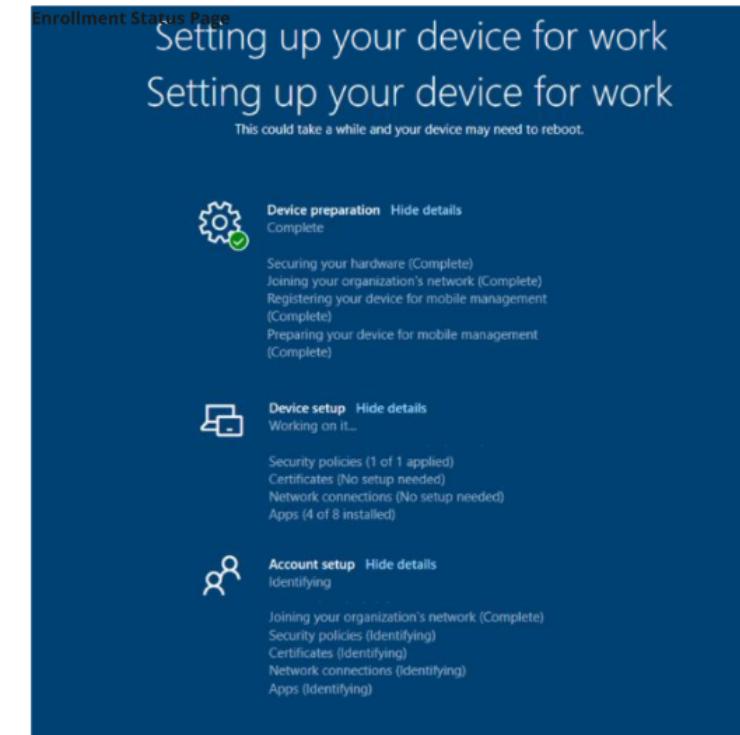
User Driven Deployment without white glove



User Driven Deployment with white glove



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

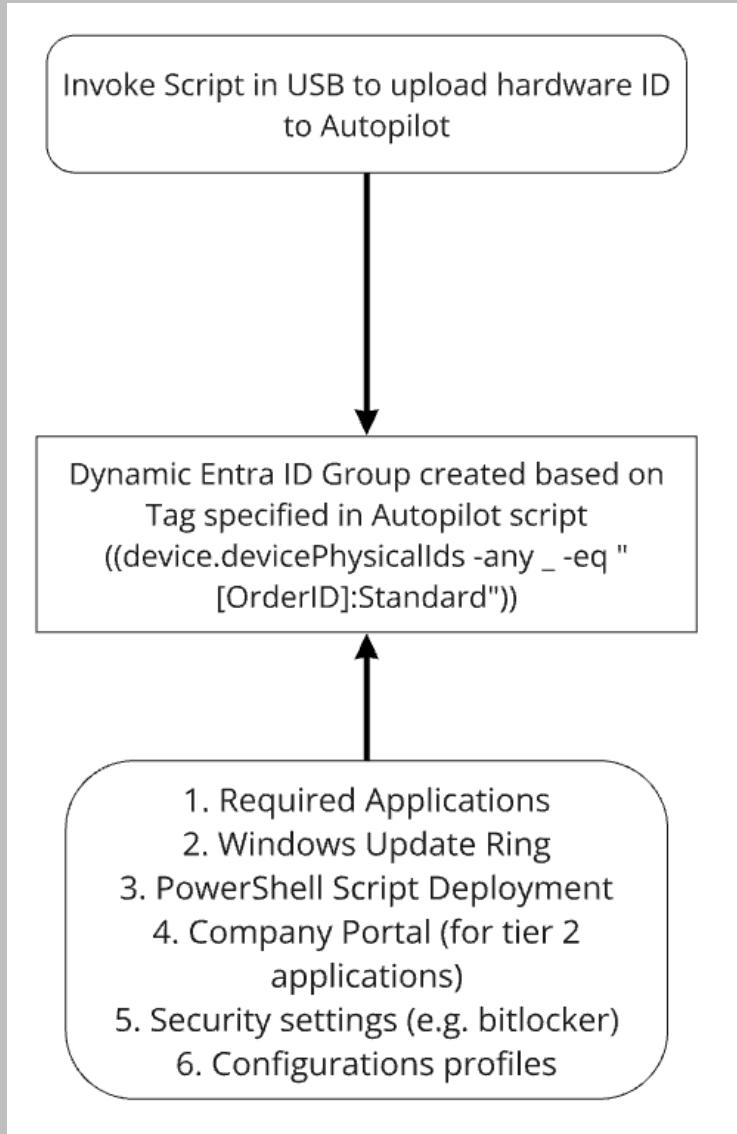
The screenshot shows the 'Dynamic membership rules' configuration page for a group named 'Intune_Standard'. The left sidebar lists 'Overview', 'Diagnose and solve problems', and several management options: Properties, Members, Owners, Roles and administrators, Administrative units, Group memberships, Applications, Licenses, and Azure role assignments. The 'Dynamic membership rules' option at the bottom of the sidebar is highlighted with a red box. The main content area is titled 'Configure Rules' and includes a 'Rule syntax' text box containing the expression '(device.devicePhysicalIds -any (_ -eq "[OrderID]:Standard"))', which is also highlighted with a red box. Below the rule syntax are tabs for 'And/Or' and 'Property', and a button for '+ Add expression'.

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: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• Admin privilege• Non-admin privilege
Decision	Non-admin privilege

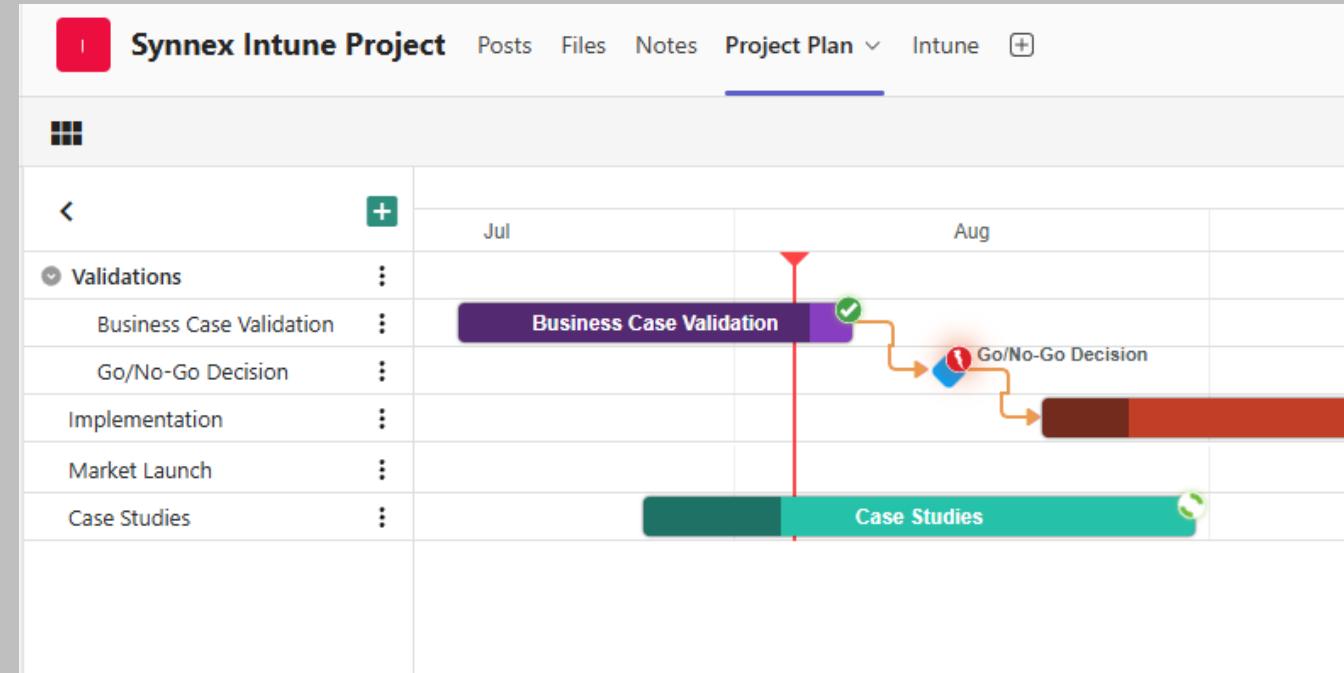
18. Wallpaper

Subject Area	Wallpaper
Topic	Discussion on wallpaper
Options	The following options will be considered: <ul style="list-style-type: none">• 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 deploy for clients.
- Reusability

<https://github.com/jseerden/IntuneBackupAndRestore>



GitHub - mtnehaus/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	
2 nd tier app can be installed via Company Portal	

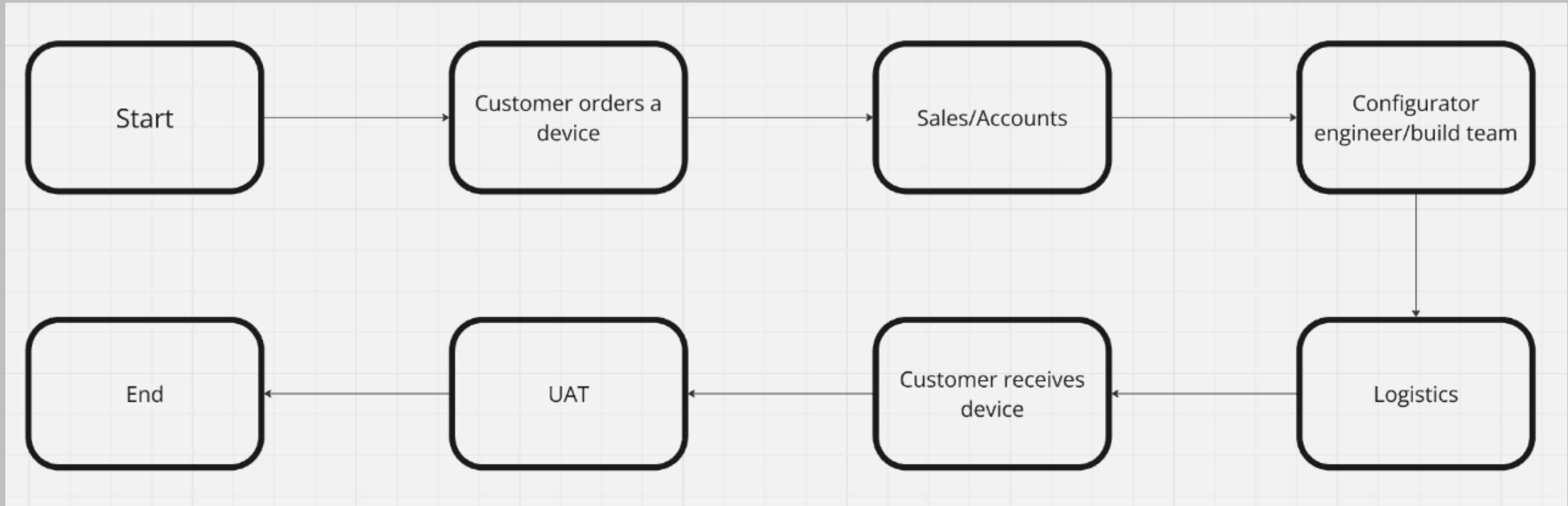
Published Applications and Scripts

Scripts for enrolment

-  [REDACTED] Architecture Decisions V1.3-Release.pdf
-  [REDACTED] As built.xlsx
-  [REDACTED] Detailed design V1.0 - Release.pdf
-  Windows 11 application deployment guide.pdf
-  Windows 11 build guide for Administrators.pdf
-  Windows 11 guide for end user.pdf
-  Windows 11 quick reference guide.pdf
-  Windows 11 UAT document.pdf

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)

Select app type

Create app

App type

Select app type

Store app

Microsoft Store app (new)

Microsoft Store app (legacy)

Microsoft 365 Apps

Windows 10 and later

Microsoft Edge, version 77 and later

Windows 10 and later

Web Application

Windows web link

Other

Web link

Line-of-business app

Windows app (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

The screenshot shows the Microsoft 365 Apps admin center with the 'Office Customization Tool' page. The left side features a navigation menu with 'Products and releases' selected. Under 'Deployment settings', there are sections for 'Architecture' (set to 64-bit), 'Products' (with dropdowns for 'Office Suites', 'Visio', 'Project', and 'Additional products'), and 'Update channel'. On the right, a 'Configured settings' panel displays various configuration items with their current status:

Category	Setting	Status
General	Provide your organization name to set the Company property on Office documents	Not configured
	Provide a description for this configuration for documentation purposes	Not configured
Products	Architecture	64-bit
	Update channel	Not configured
	Version to deploy	Not configured
Languages	Language	Not configured
	Installations options	Not configured
Installation options	Show installation to user	Full
	Shut down running applications	Off

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

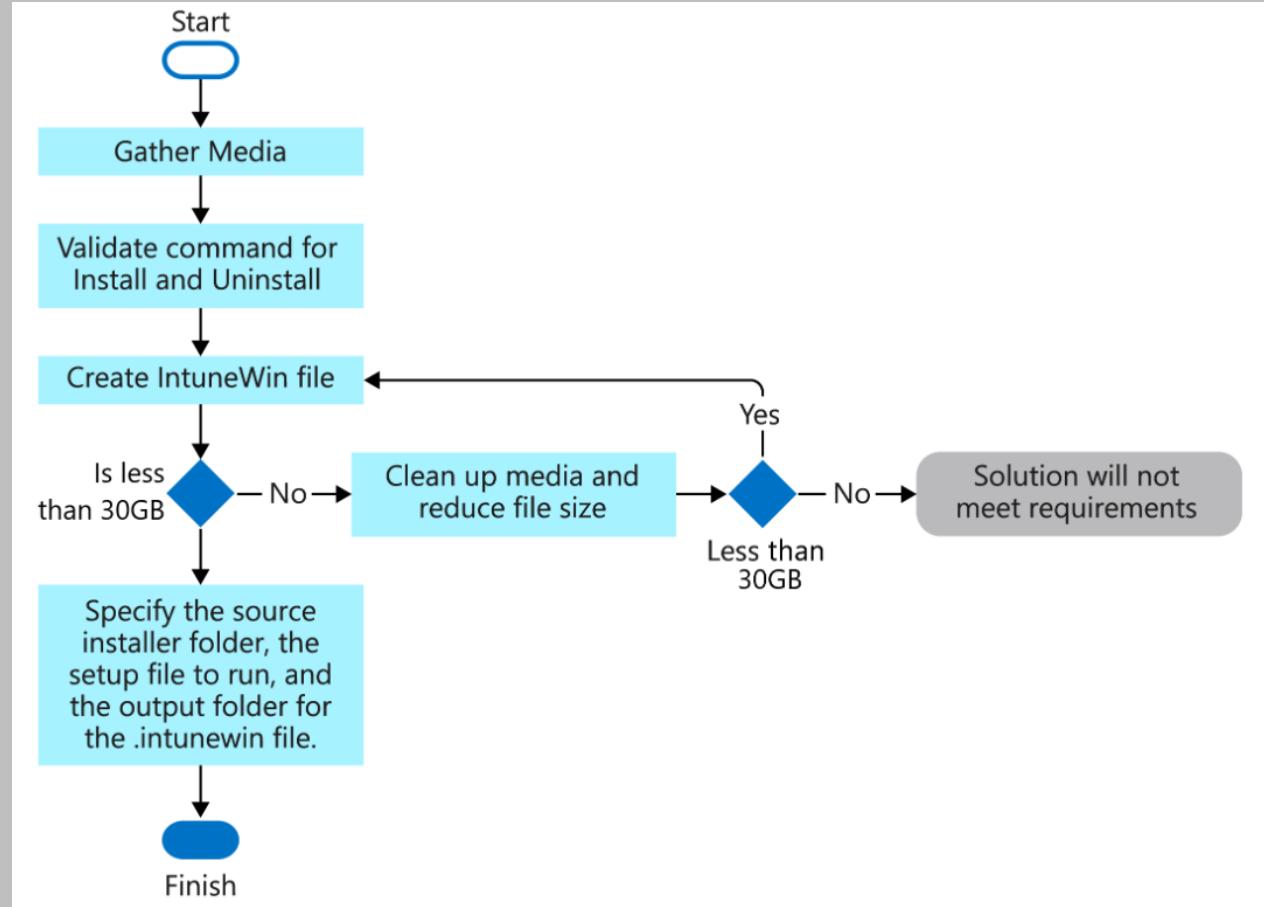
Win32 Content Prep Tool

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.

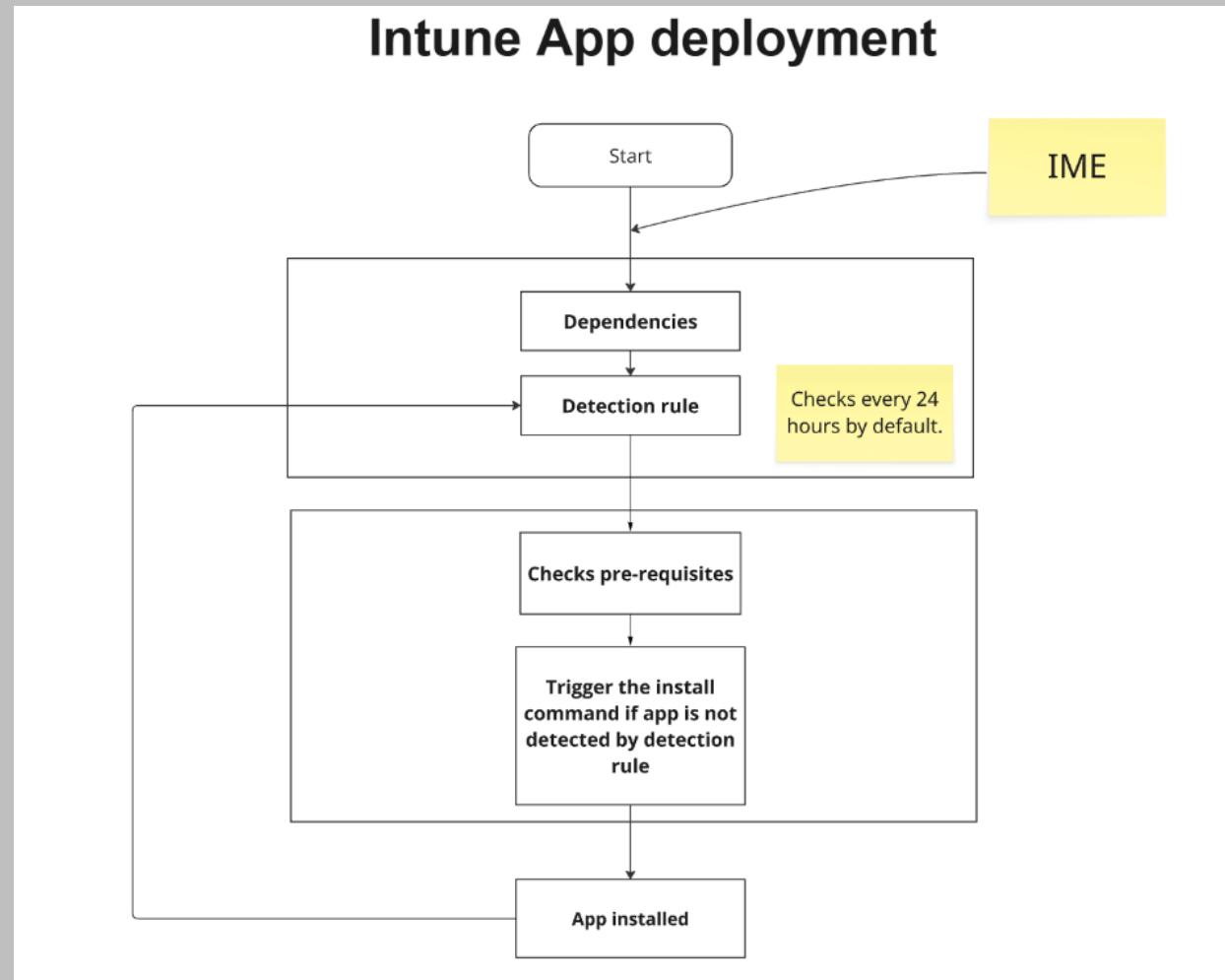
Why .msi?

- 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

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	<ul style="list-style-type: none">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	<ul style="list-style-type: none">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#understanding-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

[Home](#)[Dashboard](#)[Apps](#)

Intune policies

[+ Create](#) [⟳ Refresh](#)[🔍 Search](#)

Name	Type
<input checked="" type="checkbox"/> MDM Policy	Windows
<input checked="" type="checkbox"/> Compliance Policy	Managed device
<input checked="" type="checkbox"/> 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.

The screenshot shows the Microsoft Intune admin center interface. The left sidebar navigation includes Home, Dashboard, All services, Explorer, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. Under All services, the 'Group Policy analytics' link is highlighted with a red box. The main content area is titled 'Windows | Group Policy analytics'. It features a search bar, a 'Group policy migration readiness' section with a progress bar, and a table with columns for 'Group policy name', 'Active directory target', and 'MDM support'. At the bottom of the table, there are 'Import' and 'Migrate' buttons, with the 'Import' button also highlighted with a red box.

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.

The screenshot shows the Windows | Compliance section of the Microsoft Intune portal. On the left, there's a navigation sidebar with options like Windows devices, Monitor, Device onboarding, Manage devices, Manage updates, and Organize devices. Under Manage devices, 'Compliance' is selected. The main area displays a table with columns: Policy name, Platform or OS, Policy type, Last modified, and Scope tags. One row is visible: 'Window - Compliance policy' (Platform or OS: Windows 10 and later, Policy type: Windows 10/11 compliance p..., Last modified: 07/22/2025, 01:08 PM, Scope tags: Default). At the top of the main area, there's a note: 'One or more Threat Defense connectors are active for Windows, iOS/iPadOS, and Android but not included in an assigned compliance policy. To protect these platforms, set up a compliance policy with the Device Threat Level rule configuration in the Device Health section.'

The screenshot shows the 'Grant' configuration dialog. It has a title bar 'Grant' and a close button 'X'. Below the title, it says 'Control access enforcement to block or grant access. [Learn more](#)'. There are two radio buttons: 'Block access' (unselected) and 'Grant access' (selected). A list of controls follows, each with a checkbox and an info icon (i). The controls are:

- Require multifactor authentication
- Require authentication strength
- Require device to be marked as compliant** (This option is highlighted with a red border)
- Require Microsoft Entra hybrid joined device
- Require approved client app [See list of approved client apps](#)
- Require app protection policy [See list of policy protected client apps](#)

At the bottom, it says 'For multiple controls' with two radio buttons:

- Require all the selected controls
- Require one of the selected controls

Shared drive mapping & printer mapping

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

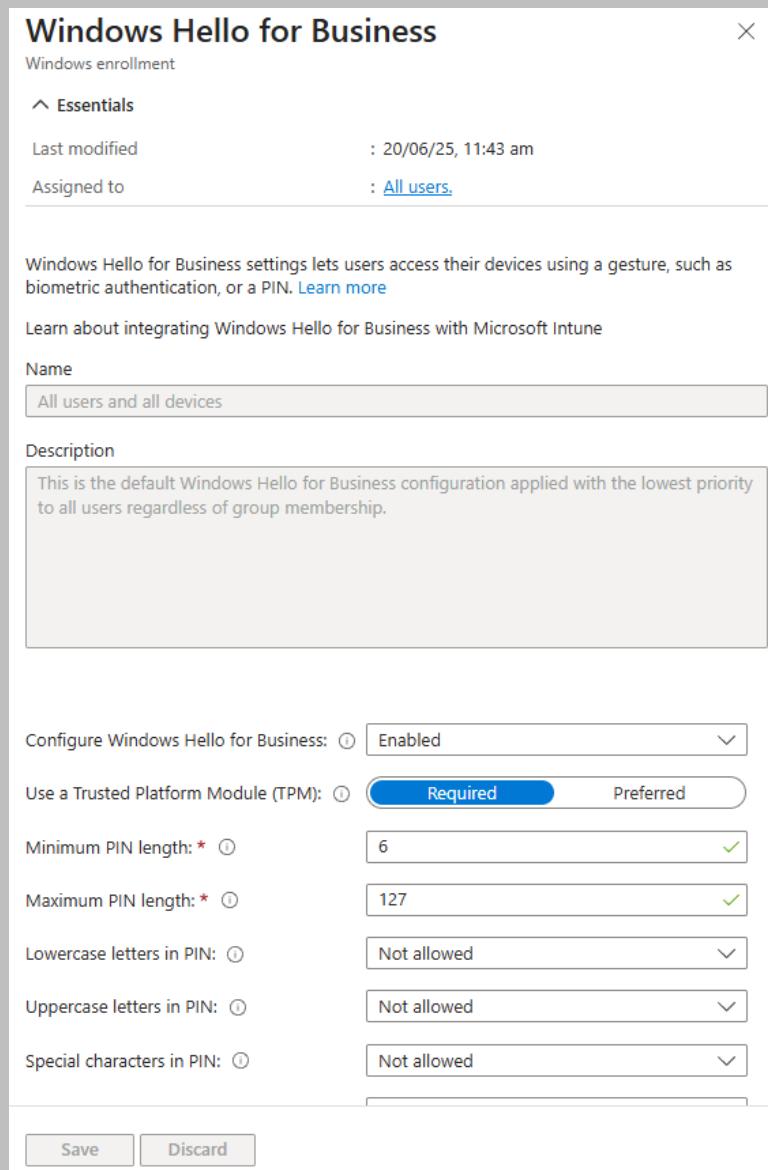
- Can we use Sharepoint online to replace shared drive?
- Can we use Teams or Azure files?
- Can we use Universal print?

<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

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

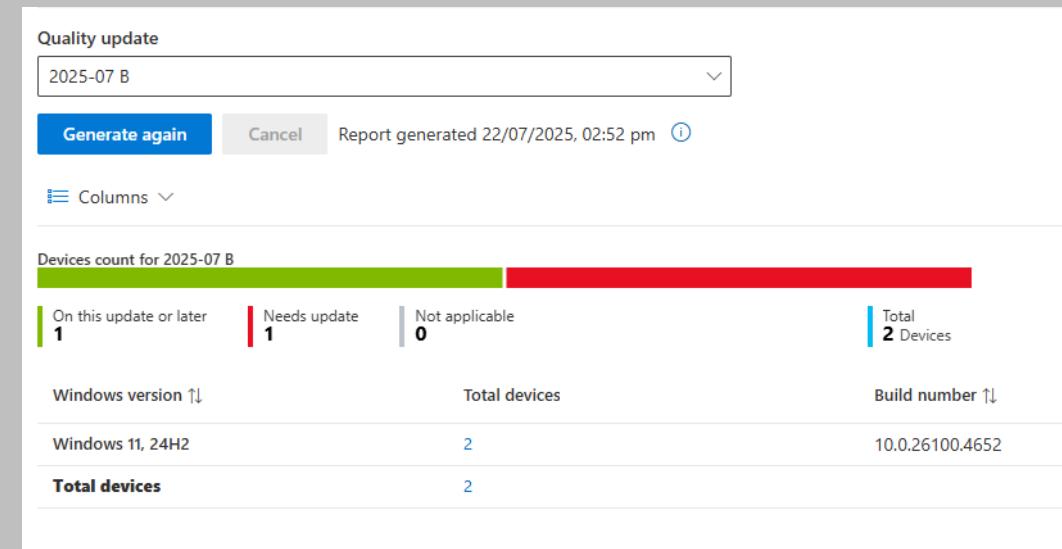
Deadline for feature updates 2

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

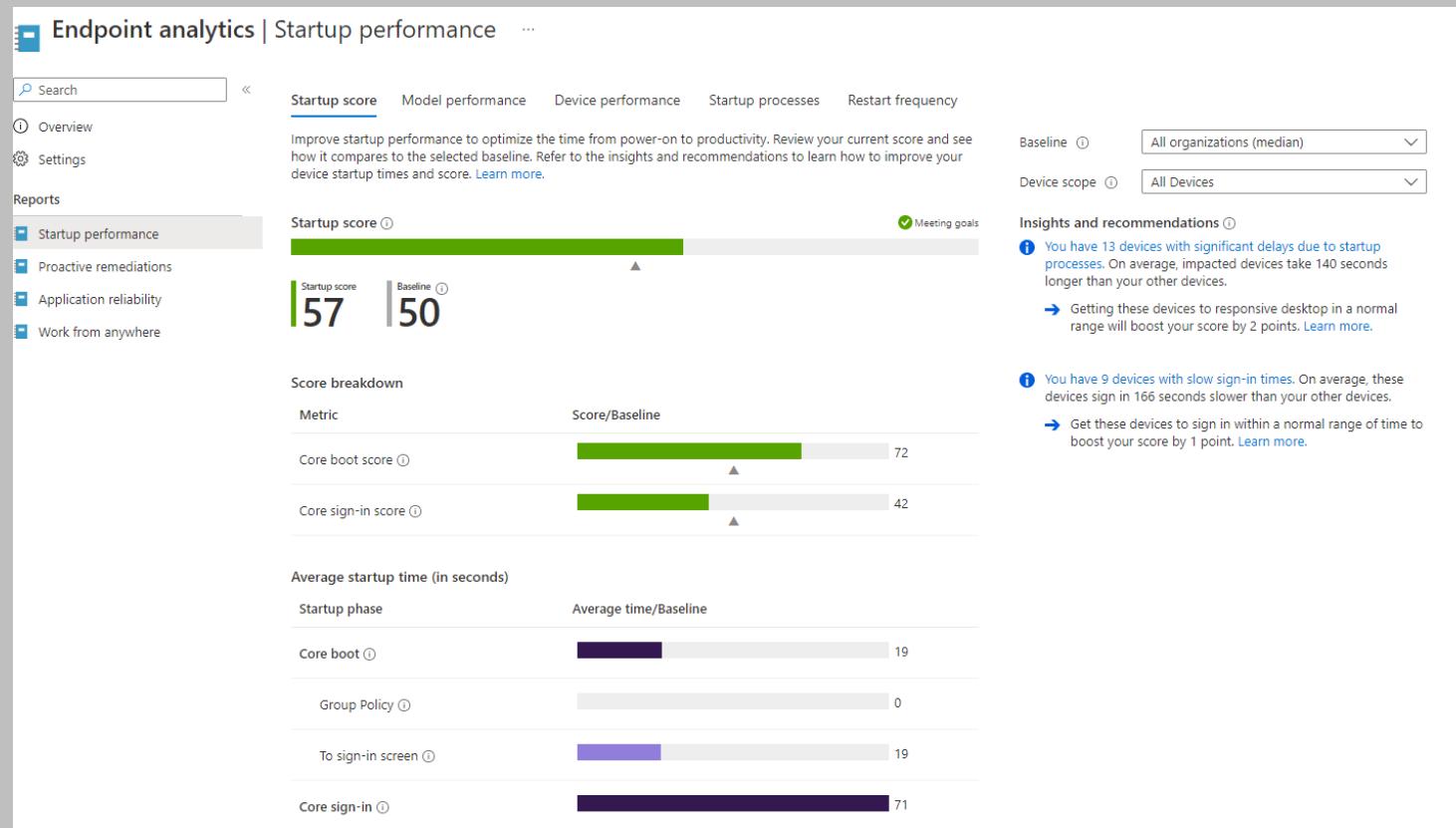
Autopatch is available with Business Premium license.
You can enable/deploy Autopatch by creating an Autopatch group

The screenshot shows the Microsoft Tenant admin interface. On the left, there's a navigation sidebar with various links like Home, Dashboard, All services, Explorer, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration (which is highlighted with a red box), and Troubleshooting + support. Under Tenant administration, there's a 'Windows Autopatch' section with 'Autopatch groups' (also highlighted with a red box). The main content area is titled 'Tenant admin | Autopatch groups'. It has a search bar and a button to '+ Create'. Below that is a table with one record:

Name	Deployment rings	Devices registered	Distribution type	Microsoft Entra groups	Scope tags	Status
Autopatch	3	0	Assigned	View details	Default	Active

Endpoint Analytics

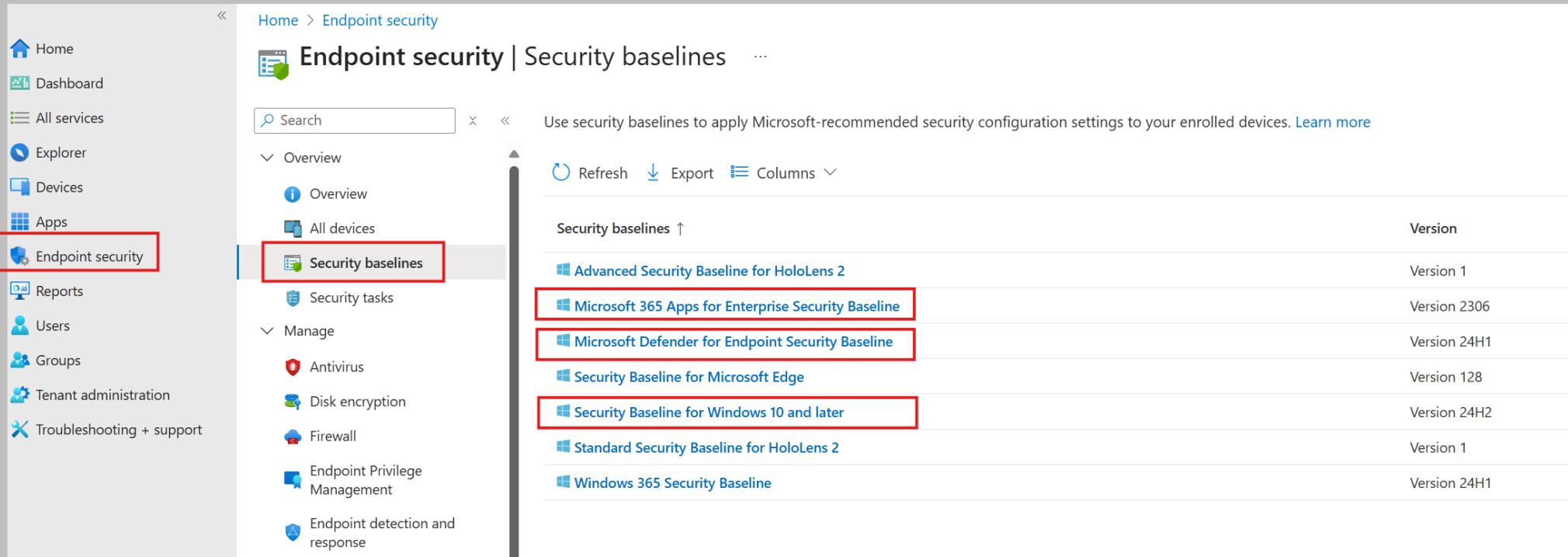
Endpoint analytics can help you to visualize the quality of the experience you're delivering to your users. Endpoint analytics can help identify policies or hardware issues that may be slowing down devices and help you proactively make improvements.



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



The screenshot shows the 'Endpoint security | Security baselines' page in the Microsoft Endpoint Manager interface. The left sidebar is titled 'Endpoint security' and includes options like Home, Dashboard, All services, Explorer, Devices, Apps, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The 'Endpoint security' option is highlighted with a red box. The main content area has a search bar and navigation buttons for Refresh, Export, and Columns. It displays a list of security baselines:

Security baselines ↑	Version
Advanced Security Baseline for HoloLens 2	Version 1
Microsoft 365 Apps for Enterprise Security Baseline	Version 2306
Microsoft Defender for Endpoint Security Baseline	Version 24H1
Security Baseline for Microsoft Edge	Version 128
Security Baseline for Windows 10 and later	Version 24H2
Standard Security Baseline for HoloLens 2	Version 1
Windows 365 Security Baseline	Version 24H1

- 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 conflicts
- Does not necessarily apply to Essential 8 – you can however modify accordingly to achieve different Essential 8 Maturity levels.

BitLocker

The screenshot shows the Microsoft Intune Endpoint security | Disk encryption interface. On the left, there's a navigation sidebar with sections like Overview, All devices, Security baselines, Security tasks, Manage, Antivirus, Disk encryption (which is highlighted with a red box), Firewall, Endpoint Privilege Management, and Endpoint detection and response. At the top right, there are buttons for 'Create Policy' (also highlighted with a red box), Refresh, and Export. Below these are search and filter options. A main table area shows columns for Policy name, Policy type, and Assigned, with a note 'No results'. To the right, a 'Create a profile' panel is open, showing fields for Platform (Windows), Profile (BitLocker), and BitLocker details. The BitLocker section includes a description of the feature, a note about policy compatibility (Windows 10 and later), and a target device note (MDM supported devices). A red box highlights the 'Create Policy' button and the BitLocker profile creation panel.

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

The screenshot shows the Microsoft Endpoint security | Account protection interface. On the left, there's a navigation sidebar with sections like Overview, Manage, and Account protection (which is highlighted with a red box). The main area displays a table of existing policies, with one row for 'LAPS 2.0' and another for 'Local admin account'. A modal window titled 'Create a profile' is open on the right, showing the 'Platform' set to 'Windows' and the 'Profile' set to 'Local admin password solution (Windows LAPS)'. This modal is also highlighted with a red box.

Policy name	Policy type	Assigned
LAPS 2.0	Local admin password soluti...	Yes
Local admin account	Local user group membership	Yes

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

Home > Endpoint security

Endpoint security | Attack surface reduction

Search x « Policies Reusable settings

Overview All devices Security baselines Security tasks

Manage Antivirus Disk encryption Firewall Endpoint Privilege Management Endpoint detection and response App Control for Business (Preview)

Attack surface reduction Account protection Device compliance Conditional access

Attack surface reduction policies

+ Create Policy Refresh Export

Search by profile name

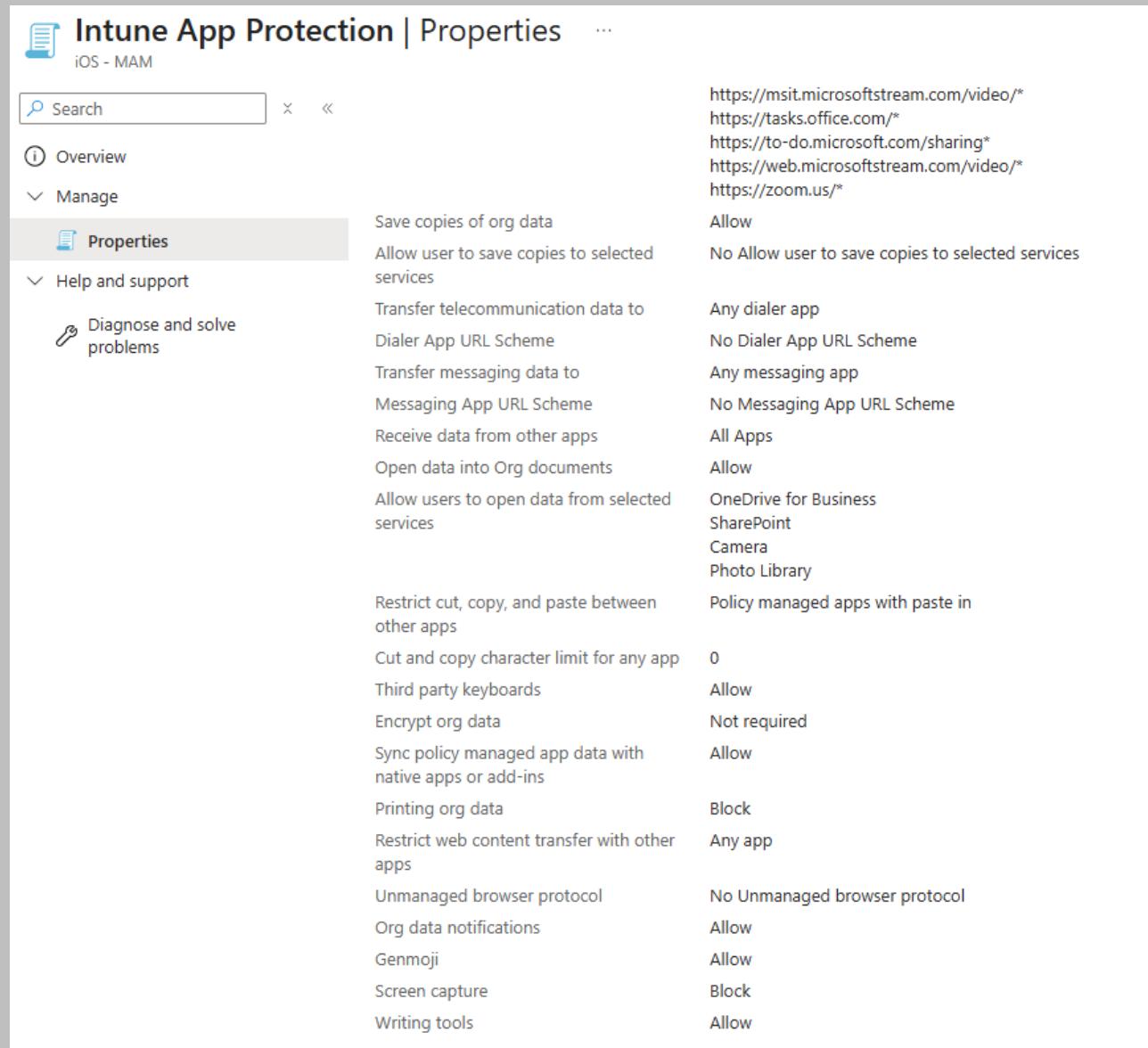
Policy name	↑↓ Policy type	↑↓ Assigned	↑↓ Platform
WDAC	Application control	Yes	Windows
ASR - Block USB	Device Control	Yes	Windows
ASR - Controlled Folder Access	Attack Surface Redu...	Yes	Windows
ASR - ML2-OM-01 - Microsoft Office macros are blocked from making Win32 API calls.	Attack Surface Redu...	No	Windows

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.

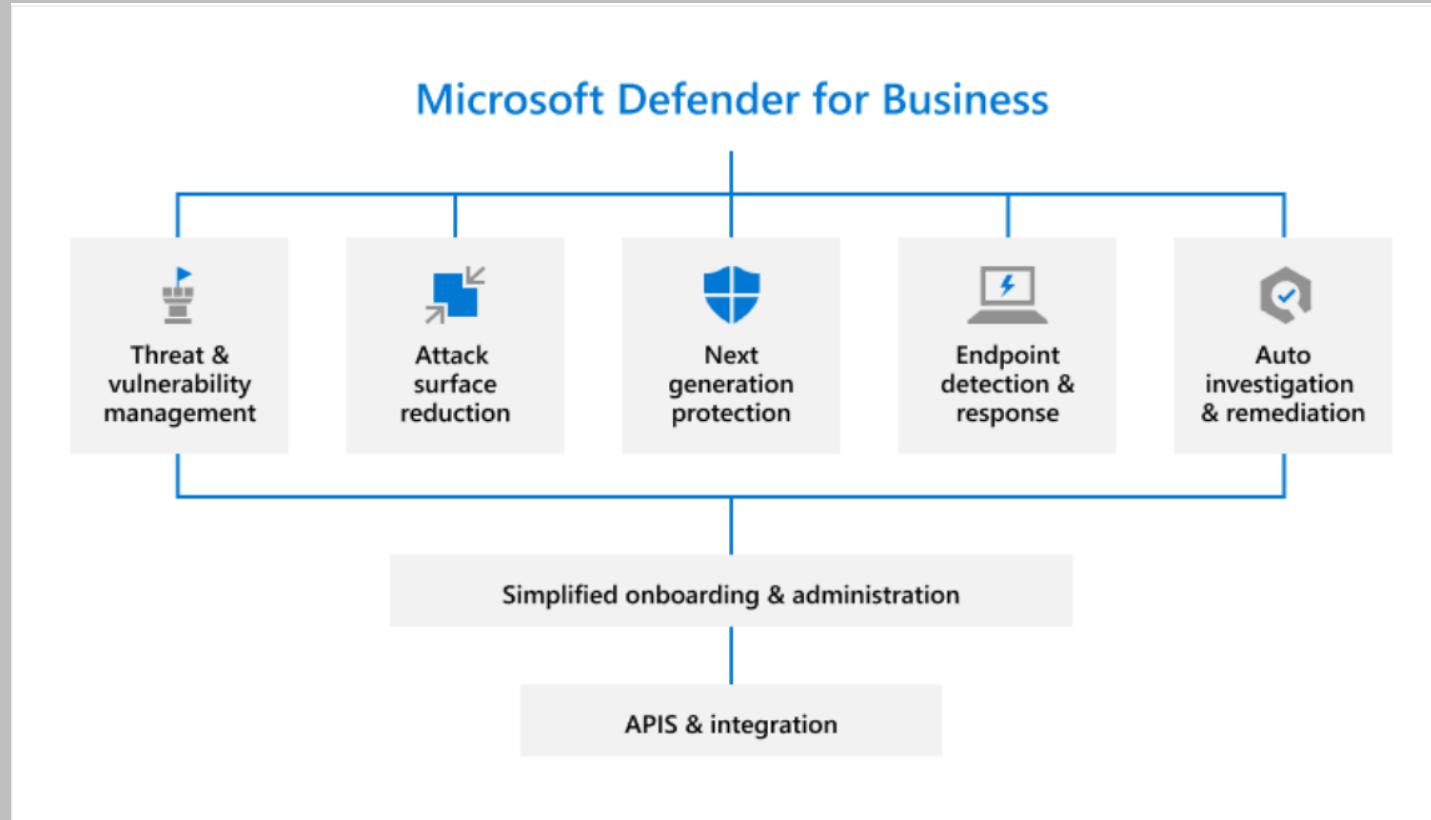


The screenshot shows the 'Intune App Protection | Properties' page for an 'iOS - MAM' configuration. The left sidebar includes 'Overview', 'Manage' (selected), 'Properties' (selected), and 'Help and support'. The 'Properties' section contains various policy settings:

Setting	Description	Value
Save copies of org data	https://msit.microsoftstream.com/video/*	Allow
Allow user to save copies to selected services	https://tasks.office.com/*	No Allow user to save copies to selected services
Transfer telecommunication data to	https://to-do.microsoft.com/sharing*	Any dialer app
Dialer App URL Scheme	https://web.microsoftstream.com/video/*	No Dialer App URL Scheme
Transfer messaging data to	https://zoom.us/*	Any messaging app
Messaging App URL Scheme	https://msit.microsoftstream.com/video/*	No Messaging App URL Scheme
Receive data from other apps	https://tasks.office.com/*	All Apps
Open data into Org documents	https://to-do.microsoft.com/sharing*	Allow
Allow users to open data from selected services	https://web.microsoftstream.com/video/*	OneDrive for Business SharePoint Camera Photo Library
Restrict cut, copy, and paste between other apps	https://zoom.us/*	Policy managed apps with paste in
Cut and copy character limit for any app	0	
Third party keyboards	https://msit.microsoftstream.com/video/*	Allow
Encrypt org data	https://tasks.office.com/*	Not required
Sync policy managed app data with native apps or add-ins	https://web.microsoftstream.com/video/*	Allow
Printing org data	https://to-do.microsoft.com/sharing*	Block
Restrict web content transfer with other apps	https://zoom.us/*	Any app
Unmanaged browser protocol	https://msit.microsoftstream.com/video/*	No Unmanaged browser protocol
Org data notifications	https://tasks.office.com/*	Allow
Genemoji	https://web.microsoftstream.com/video/*	Allow
Screen capture	https://zoom.us/*	Block
Writing tools	https://msit.microsoftstream.com/video/*	Allow

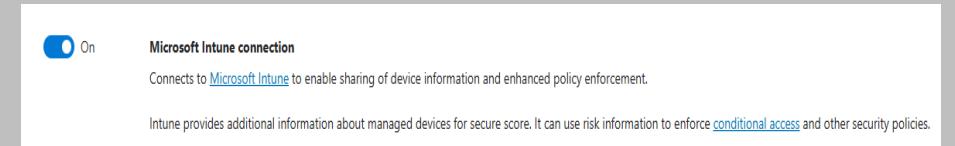
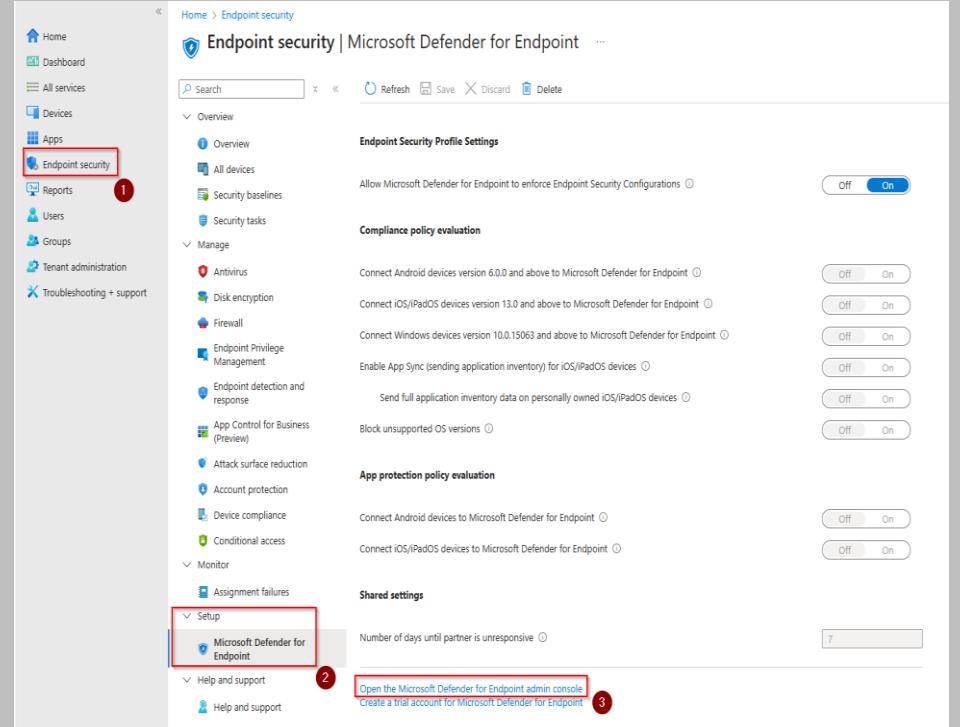
Microsoft Defender for Endpoint

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

Microsoft Defender Vulnerability Management dashboard

Organization exposure score

Exposure score

This score reflects the current exposure associated with devices in your organization. The score is potentially impacted by active exceptions.

63/100

Low 0-29 Medium 30-69 High 70-100

Exposure score over time

Improve score

Top security recommendations

Recommendation	Exposed devices	Actions
Update Microsoft Windows 11 (OS and b...)	6	0
Update Microsoft Edge Chromium-base...	4	0
Update Microsoft Office	6	0

Show more Show exceptions

Microsoft Secure Score for Devices

Your score for devices: 69%

This score reflects the collective security configuration posture of your devices across OS, Application, Network, Accounts and Security Controls Score is potentially impacted by active exceptions.

526/765 points achieved

Category	Score / Total
Application	3 / 20
OS	170 / 191
Network	76 / 98

View in map Device value ...

- Set criticality
- Manage tags
- Report device inaccuracy
- Run Antivirus Scan
- Collect Investigation Package
- Restrict App Execution
- Initiate Automated Investigation
- Initiate Live Response Session
- Isolate Device
- Action center
- Download force release from isolation script
- Exclude
- Go hunt
- Turn on troubleshooting mode
- Policy sync

Compliance Manager

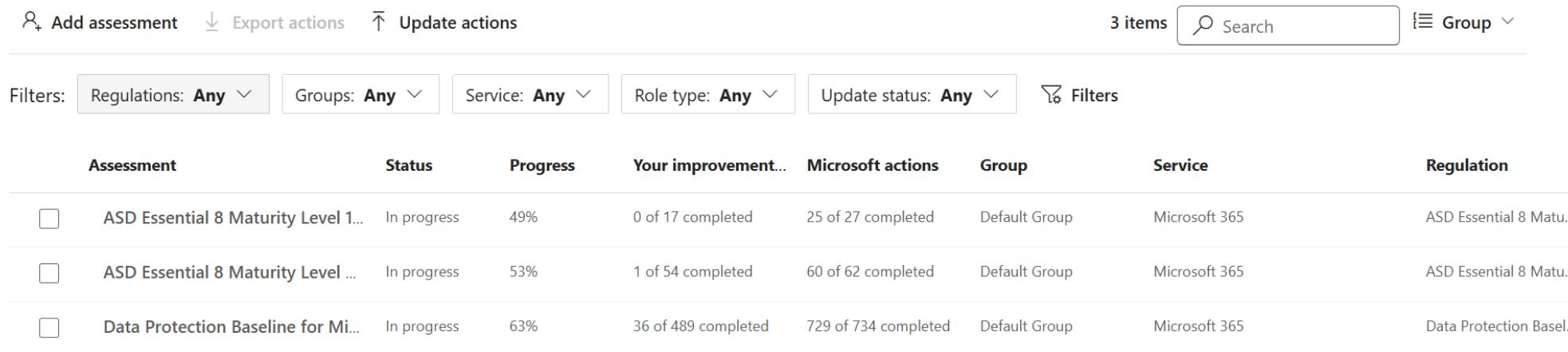
Microsoft Purview Compliance Manager is a solution that helps you automatically assess and manage compliance across your environment. Compliance Manager can help you stay current with regulations and reporting to auditors.

Assessments

Assessments help you implement data protection controls specified by compliance, security, privacy, and data protection standards, regulations, and laws. Assessments include actions that have been taken by Microsoft to protect your data, and they're completed when you take action to implement the controls included in the assessment. [Learn how to manage assessments](#)

Free regulation licenses used | Purchased regulation licenses used
1/3 | **0/0**

[View details](#)



The screenshot shows the Microsoft Purview Compliance Manager interface for managing assessments. At the top, it displays two counts: 'Free regulation licenses used' (1/3) and 'Purchased regulation licenses used' (0/0). Below this, there's a link to 'View details'. The main area features a table with columns for Assessment, Status, Progress, Your improvement..., Microsoft actions, Group, Service, and Regulation. Each row in the table represents a different assessment, such as 'ASD Essential 8 Maturity Level 1...' or 'Data Protection Baseline for Mi...'. The table includes filters at the top and a search bar. The bottom of the table shows three items found and a 'Search' button.

Assessment	Status	Progress	Your improvement...	Microsoft actions	Group	Service	Regulation
<input type="checkbox"/> ASD Essential 8 Maturity Level 1...	In progress	49%	0 of 17 completed	25 of 27 completed	Default Group	Microsoft 365	ASD Essential 8 Matu...
<input type="checkbox"/> ASD Essential 8 Maturity Level ...	In progress	53%	1 of 54 completed	60 of 62 completed	Default Group	Microsoft 365	ASD Essential 8 Matu...
<input type="checkbox"/> Data Protection Baseline for Mi...	In progress	63%	36 of 489 completed	729 of 734 completed	Default Group	Microsoft 365	Data Protection Basel...

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.

Sensitivity labels

i You can now create sensitivity labels with privacy and access control settings for Teams, SharePoint sites, and Microsoft 365 Groups. To do this, you must first [complete these steps](#). Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is encrypted, files are added to content marking, and user access to specific sites. [Learn more about sensitivity labels](#)

+ Create a label  Publish labels  Export  Refresh

<input type="checkbox"/>	Name	Priority	Scope	Created by
<input type="checkbox"/>	General - Non sensitive information	0	Files & other data assets, Email, Mee...	Ted Zhang
<input type="checkbox"/>	Confidential	1	Files & other data assets, Email, Mee...	Ted Zhang
<input type="checkbox"/>	Highly Confidential	2	Files & other data assets, Email, Mee...	Ted Zhang

Protect sensitive data referenced in Copilot and agent responses

Sensitivity labels help protect files by controlling user access to data. Microsoft 365 Copilot and agents honor sensitivity labels on files and only show users files they already have access to in prompts and responses. Use data risk assessments to identify potential oversharing risks, including unlabeled files.

Unlabeled files in Copilot and agent interactions

5	Unlabeled files	2	SharePoint Sites with unlabeled files
--	-----------------	--	---------------------------------------

Top 2 SharePoint sites with unlabeled files in Copilot and agent interactions



[View top 2 sites](#)

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.

Policies

Use data loss prevention (DLP) policies to help identify and protect your organization's sensitive info. For example you can set up policies to help make sure information in email and docs isn't shared with the wrong people. [Learn more about DLP](#)

⚠ Some of your devices are in not updated state. [Go to onboarding devices to see more details](#)

⚠ Set up billing to continue protecting activity in Fabric. Support for Fabric in DLP is now a pay-as-you-go capability. Existing policies scoped to Fabric will work for a short time, but you can't edit them or create new ones for Fabric until you link an Azure subscription for billing. Policies scoped to other sources aren't linked to the pay-as-you-go billing model. [Learn more about pay-as-you-go billing](#)

[Get started](#)

<input type="checkbox"/> Name	Priority	Mode	Policy sync status	Last modified
<input type="checkbox"/> Highly Confidential	0	On	✓ Sync completed	May 23, 2025 12:55 PM
<input type="checkbox"/> Prevent Copilot using documents marked as Confidential	1	On	✓ Sync completed	Jun 26, 2025 4:51 PM
<input type="checkbox"/> Australia Financial Data	2	Test with notifications	✓ Sync completed	Apr 28, 2025 5:13 PM
<input type="checkbox"/> DSPM for AI: Detect sensitive info added to AI sites	3	On	✓ Sync completed	May 1, 2025 12:30 PM
<input type="checkbox"/> Custom policy	4	Test with notifications	✓ Sync completed	Jun 5, 2025 3:17 PM
<input type="checkbox"/> DLP for sharepoint external sharing	5	On	✓ Sync completed	Jun 26, 2025 4:28 PM
<input type="checkbox"/> test auto labeling	6	On	✓ Sync completed	Jul 4, 2025 3:37 PM

7 items



Search



Customize columns

What's my starting point?



**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/>