

Microsoft Intune and Autopilot

Enrolling and managing Windows, macOS, iOS, and Android in a cloud-first estate.

About this session

Microsoft Intune simplifies device deployment and management across Windows, macOS, iOS, and Android. This session provides a practical overview of the device enrollment process, including enrollment methods, enrollment profiles, identity integration with Microsoft Entra ID, compliance policies, and best practices. Attendees will gain the knowledge needed to successfully enroll and manage devices in a modern cloud-first environment.

Who this is for

Target audience

IT professionals responsible for deploying, enrolling, and managing organizational devices using Microsoft Intune: desktop support technicians, systems administrators, endpoint administrators, help desk staff, and IT managers who are new to Intune or looking to strengthen their knowledge of device enrollment and modern device management.

Knowledge requirements

An understanding of Entra, meaning groups, users, and conditional access policies, and a general understanding of endpoint management.

Skill level

Intermediate.

Learning objectives

Describe the different Microsoft Intune device enrollment methods for Windows, macOS, iOS, and Android devices and determine when to use each.

Configure the components required for successful device enrollment, including Microsoft Entra ID integration, enrollment profiles, compliance policies, and licensing considerations.

Troubleshoot common enrollment issues and apply best practices for securely onboarding devices into Microsoft Intune.

Contents

- 01 Modern endpoint management
- 02 Entra ID foundations
- 03 Windows enrollment methods
- 04 Windows Autopilot
- 05 macOS, iOS, and Android
- 06 Compliance and Conditional Access
- 07 Troubleshooting
- 08 Features worth taking home

BEFORE WE START

How this runs

Interrupt with questions.

Anything we cannot answer straight away goes on the parking lot and gets answered before we finish.

If you would like to review a feature, topic, or idea outside of this presentation, just ask after the session and I will be glad to take a look.

01

Modern endpoint management

From imaging to enrollment

The device configures itself from the cloud instead of being built from an image.

Identity, not the network, decides what a device gets. No line of sight to a domain controller.

Configuration is policy that keeps converging, not a state captured once at build time.

Enrollment is the moment a device gains identity, policy, and management. Everything follows from it.

Show of hands

Which of these is doing the most work in your estate this morning?

Group Policy

Domain joined, configured by Group Policy, imaged at the bench.

Configuration Manager

Task sequences, distribution points, and a maintenance window.

Intune

Some or all of the estate enrolled and managed from the cloud.

Where Intune sits

Microsoft Entra ID

Identity: users, groups, device objects, and Conditional Access. The prerequisite for everything else.

Microsoft Intune

Device and app management: enrollment, configuration, compliance, apps, updates, and remediation.

Defender and Purview

Risk and data signals that feed compliance and access decisions back into Intune and Entra.

Co-management or cloud-native

Configuration Manager only

On premises, domain joined, image based. Fine on the office network, hard for remote staff and new hardware.

Tenant attach

Existing Configuration Manager devices shown in the Intune console for actions and reporting. Low risk.

on-premises authority

Cloud-native

Joined to Entra ID, provisioned by Autopilot, managed by Intune. No image and no domain join.

Co-management

Both authorities on one device, with workloads moved to Intune one at a time. The migration path.

cloud authority

Platform coverage at a glance

PLATFORM	CORPORATE PATH	PERSONAL PATH	IDENTITY
Windows	Autopilot, join to Entra ID	Registration, app management	Joined or hybrid joined
macOS	Automated Device Enrollment	Company Portal enrollment	Registered
iOS and iPadOS	Automated Device Enrollment	User enrollment, apps only	Registered
Android	Fully managed, dedicated	Work profile, apps only	Registered

Module 01 in short

Cloud management replaces the image with policy the device pulls for itself.

Identity decides what a device receives, which is why module 02 is about Entra ID.

Co-management and tenant attach are routes from where you are to cloud-native.

Every platform follows the same three steps: connect, declare a profile, enroll.

02

Entra ID foundations

Enrollment is an identity event

The user must exist in Entra ID and hold a licence that includes Intune.

The user must be inside the device management scope for automatic enrollment.

The device platform and version must be allowed by your enrollment restrictions.

Nothing in Conditional Access may block the enrollment endpoints for that user.

Three device identity states

Registered

A personal or unmanaged device with a work identity added. Common for personal phones and laptops.

Joined

A corporate device whose primary identity lives in the cloud. The target state for Windows under Autopilot.

Hybrid joined

Joined to on-premises Active Directory and synchronised to Entra ID.
Supported, but not for new hardware.

Groups that carry the deployment

Assigned groups

Explicit membership. Predictable and instant, which is what you want for pilot rings and for anything you are about to demonstrate in front of people.

Rule-based device groups

Membership from a rule: order number, group tag, model, or enrollment profile name. These scale, but evaluation takes time and profile assignment waits on it.

Decide the names once

01

Groups

Purpose, platform, ring. A name like INT-WIN-Pilot reads the same to everyone in a year.

02

Group tags

One per hardware batch or per site. This is what steers a device to a profile.

03

Profiles

Platform, join type, and mode in the name, so an assignment explains itself.

04

Devices

A short prefix plus the serial number. Fifteen characters, no spaces, no department names.

Automatic enrollment settings

SETTING	WHERE	WHAT IT DOES
Device management scope	Entra ID, Mobility	Who may enroll automatically when a device is joined
App management scope	Entra ID, Mobility	App-level management for personal Windows devices
Platform restrictions	Intune, Enrollment	Allows or blocks platforms, versions, personal devices
Device limit	Intune, Enrollment	How many devices one user may enroll
Corporate identifiers	Intune, Enrollment	Serial or hardware numbers that mark a device as company owned

Restrictions in practice

Restrictions apply at enrollment time only. Tightening one never removes a device already managed.

Blocking personally owned devices per platform is the single most useful restriction.

A minimum operating system version keeps unpatchable hardware out without a conversation.

Device limits count retired objects until they are deleted, so clean up quarterly.

Licensing, in practical terms

YOU NEED	COMES FROM	NOTE
Intune Plan 1	Standalone, Microsoft 365 E3 or E5, Business Premium	Baseline device and app management, per user
Entra ID P1	Microsoft 365 E3 or E5, Business Premium	Conditional Access and rule-based groups
Intune Plan 2 or Suite	Add-on	Remote Help, privilege management, advanced analytics
Device licences	Add-on	Shared and kiosk devices with no assigned user

DEMO · 15 MIN

A tour of the tenant

Devices, enrollment, and restriction blades

Mobility settings and the device
management scope

Where a device object appears after
enrollment

Company Portal branding

Tenant readiness check

01

Confirm licensing

Check that your account and your test user both hold an Intune licence.

02

Set the scope

Point the device management scope at a group rather than at everyone, and add your test user.

03

Brand the portal

Add a name, a support contact, and a colour to Company Portal.

04

Find the blades

Locate Devices, Enrollment, and Troubleshooting and support without using the search box.

Groups and restrictions

01

Write the names

Agree your own convention for groups, tags, profiles, and device names.

02

Build three rings

Pilot, early, and broad, as assigned groups, with yourself in pilot.

03

One rule-based group

Write a rule on an Autopilot group tag and note how long membership takes.

04

Restrict a platform

Block personally owned devices on one platform and record the message a user sees.

Module 02 in short

Enrollment needs a licensed user, inside the management scope, on an allowed platform.

Assigned groups for anything time sensitive, rule-based groups for anything at scale.

Restrictions apply at enrollment only, so decide your posture before you enroll anything.

Names and group tags are cheap now and expensive later. Write them down today.

03

Windows enrollment methods

Five ways a Windows device enrolls

METHOD	BEST FOR	REQUIRES
Autopilot	New or reset corporate hardware	A registered device and a deployment profile
Join at first-boot setup	Small batches built by a technician	Management scope and a licence
Group Policy enrollment	An existing hybrid joined estate	Hybrid join, Group Policy, network line of sight
Co-management	A Configuration Manager estate in transition	Configuration Manager and cloud attach
Personal device registration	Personal devices that need work apps	Device or app management scope

Choosing a method

New hardware, no domain need

Autopilot, user driven, joined to Entra ID. Ship it to the user and the device builds itself.

Existing estate, domain joined

Group Policy enrollment or co-management. Enroll in place, then move workloads.

New hardware, domain need

Autopilot with hybrid join where a legacy dependency requires Active Directory, and a plan to retire it.

Personal device

App management, with or without registration. Manage the data rather than the hardware.

Hybrid join: when, and when not

Reasonable reasons

An application that authenticates only to Active Directory, print or file paths bound to on-premises authentication, or a certificate estate you cannot yet reissue from the cloud.

What it costs

Network line of sight to a domain controller during setup, a connector and an organizational unit to maintain, and a longer first boot with more places to fail.

Bulk and technician paths

Provisioning packages

Windows Configuration Designer produces a package applied during first-boot setup. Useful where registration is not possible.

Bulk enrollment

A provisioning package carrying an enrollment token, joining devices under a device-only account.

Pre-provisioning

The Autopilot technician flow, where policy and apps land before the user ever sees the device.

DISCUSSION

Talk me through yours

If you bought fifty laptops tomorrow, what actually happens to them?

Who touches them

The bench, a technician, a vendor, or nobody at all?

How long

Hours per device, or minutes?

Module 03 in short

New hardware means Autopilot. An existing domain joined estate means enroll in place.

Hybrid join is a supported answer to a specific dependency, not a default.

Provisioning packages cover the hardware your procurement process never registered.

Personal devices are an app management question, not an enrollment question.

04

Windows Autopilot

What Autopilot is, and is not

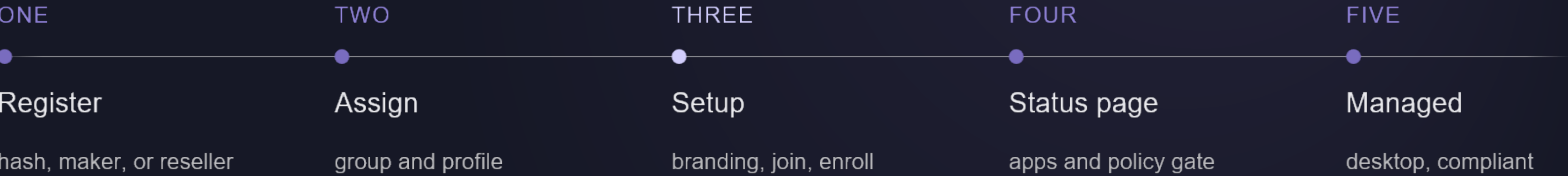
It is

A cloud service that recognises a registered device during first-boot setup, applies your branding and settings, joins it to Entra ID, and hands it to Intune for configuration.

It is not

An imaging or operating system deployment tool. Windows is already on the device. Autopilot changes what happens on first boot, not what is installed underneath.

The flow, end to end



Stage three is where most failures appear, because it is the first stage that depends on everything set up in stages one and two.

What has to be true first

A supported Windows edition, freshly installed or reset, sitting at the first-boot setup screen.

Working internet access at that screen, with the Autopilot and Intune services reachable.

The device registered, and a deployment profile assigned to a group it belongs to.

A licensed user inside the management scope, and no restriction blocking the platform.

Getting devices registered

PATH	HOW	USE WHEN
Maker or reseller	The vendor registers on your behalf at purchase	Standard for new procurement
Hardware hash upload	A script collects the hash into a spreadsheet you import	Labs, existing stock, one-off machines
Convert an enrolled device	Register a device already managed by Intune	Reusing hardware you already manage
Group tags	An attribute written on the registration record	Steering devices to profiles

Group tags earn their keep

What they are

A free text attribute on the Autopilot registration record, editable after the fact, that rule-based device groups can filter on.

What they buy you

Steering one shipment to the kiosk profile and another to the staff profile without opening a box, and re-steering a device later by editing one field.

Deployment profile modes

01

User driven

The user signs in at first boot and becomes the primary user.
The default for staff laptops.

02

Pre-provisioned

A technician runs the slow part first, and the user finishes in minutes.

03

Self deploying

No user credentials at all.
Kiosks, displays, and shared meeting room devices.

04

Reset and reuse

Autopilot reset returns a device to its assigned profile without leaving management.

The settings that bite

Join type, cloud or hybrid. Changing it later means redeploying the device.

User account type, standard or administrator. Standard, unless you can justify otherwise.

Device name template. Decide the convention before the first batch ships.

Language, region, and keyboard. Preset them or the user will be asked.

Allow pre-provisioning. Required for the technician flow and harmless if unused.

The Enrollment Status Page

What it does

Holds the desktop until the apps and policies you nominate have applied, so the user never meets a half configured machine.

How it goes wrong

Too many blocking apps, a timeout shorter than the slowest install, or permission to continue on failure that quietly hides a broken deployment.

Four status page decisions

SETTING	SENSIBLE DEFAULT	WHY
Show app and profile progress	Yes	The user can see the device is working
Block use until apps install	A short, named list	Only what a user cannot start without
Timeout	Above your measured worst case	Give Autopilot ample time to install everything
Allow use on failure	A deliberate choice either way	Yes hides breakage, no strands users

Pre-provisioning, step by step

01

Technician flow

Press the Windows key five times at the setup screen, then provision. The device does the slow work on the bench.

02

Device targeted policy

Only device scoped apps and settings apply in this phase, so plan assignments accordingly.

03

Reseal

The device returns to the setup screen, configured, ready to ship or shelve.

04

User phase

The user signs in and gets their own apps in minutes rather than hours.

Device preparation policies

Microsoft's newer Autopilot experience replaces hardware hash registration with a device preparation policy targeted at a device group, and gives a shorter, more transparent setup sequence. It coexists with the classic profile based flow. Check current platform support and feature parity before you move a production rollout onto it, and keep the classic path for the scenarios it does not yet cover.

Reset, wipe, and recovery

ACTION	KEEPS	USE FOR
Autopilot reset	Enrollment and profile	Handing a device to the next user
Wipe	Nothing	Returning to stock, or a lost device
Fresh start	User data, optionally	Clearing preinstalled vendor software
Retire	Personal data	Removing management from a personal device

DEMO · 30 MIN

Build it, then deploy it

Import a hardware hash and set a group tag

Create the rule-based group and the profile

Configure the status page and one blocking app

Watch a device go from setup screen to desktop

Register and assign

01

Collect a hash

Run the collection script on your test device and export the spreadsheet.

02

Import and tag

Upload it, set a group tag, and watch the rule-based group pick the device up.

03

Create a profile

User driven, joined to Entra ID, standard user, with a naming template.

04

Confirm assignment

Check the device shows the profile as assigned before you reset it.

Done early? Add a second group tag and a second profile, and prove one device can be re-steered by editing one field.

Deploy a device, end to end

01

Set the status page

One blocking app, a generous timeout, and progress shown to the user.

02

Reset the device

Back to the setup screen, on a network that can reach the service.

03

Sign in and watch

Note every screen the user sees. Time the run and write the number down.

04

Verify

Device object, primary user, applied policies, and compliance state.

Module 04 in short

Autopilot changes first boot. It does not install Windows.

Register, assign, then boot. A problem in the first two shows up as a failure in the third.

Group tags steer hardware to profiles without anyone touching the device.

The status page is a gate. Keep the blocking list short and the timeout honest.

05

macOS, iOS, and Android

Every platform, three steps

Connect

A trust between Intune and the platform vendor. A push certificate for Apple, managed Google Play for Android.

Declare

An enrollment profile that says what kind of device this is and how much control you take.

Enroll

Zero touch for hardware you bought through the vendor program, user initiated for everything else.

Apple: three tokens to keep alive

TOKEN	PURPOSE	RENEWAL
Push notification certificate	Lets Intune contact any Apple device	Annual. Expiry stops all Apple management
Device enrollment token	Links Apple Business Manager to Intune	Annual, per token
Apps and books token	App licences purchased through Apple	Annual

Put all three renewal dates in a shared calendar with a month of warning.

Apple enrollment types

TYPE	OWNERSHIP	CONTROL
Automated Device Enrollment	Company owned, bought through Apple Business Manager	Supervised, cannot be removed, zero touch
Apple Configurator	Company owned, existing stock	Supervised, needs a cable and a Mac
Device enrollment	Either	Full device profile, user initiated, removable
User enrollment	Personal	Work data separated, limited device control
App protection only	Personal	No enrollment. Policy applies inside the apps

macOS, specifically

FileVault

Turn on disk encryption and escrow the recovery key through Intune, then you can retrieve it later when needed.

Platform single sign-on

Entra ID sign-in at the Mac login window, with the local account tied to cloud identity.

Shell scripts

The escape hatch for anything the settings catalog does not cover yet. Use sparingly and log everything.

Android, by scenario

SCENARIO	ENROLLMENT	NOTES
Staff issued phone	Fully managed	Company owned, whole device under policy
Shared or single purpose	Dedicated	Locked to one app or a small set, no user identity needed
Company device, personal use	Work profile on a company device	Separation on hardware you own
Personal phone	Work profile	A work container only. The user keeps the device
Minimal footprint	App protection only	No enrollment at all

Managing data, not devices

App protection policies

Encryption, a required PIN, limits on copying data out, and removal of company data, all applied inside the apps, with no enrollment and no device inventory.

Why it lands well

No agent on a personal phone, no photo library in your inventory, and a much shorter conversation with the union, the council, and the privacy officer.

Enroll something that is not Windows

01

Pick a path

A work profile on Android, or
Company Portal on iOS.

02

Enroll

Note every consent screen the
user sees.

03

Inspect

Find the device in Intune and
see what you can and cannot
read about it.

04

Remove it

Retire the device and confirm
what stayed behind on the
phone.

Module 05 in short

Connect to the vendor, declare a profile, then enroll. The same three steps everywhere.

Three Apple tokens expire annually, and one of them stops all Apple management.

Android needs the managed Google Play connection before any profile works.

For personal phones, managing the data usually beats managing the device.

06

Compliance and Conditional Access

Anatomy of a compliance policy

Rules

Encryption, minimum operating system version, password or PIN, firewall, threat signals, and jailbreak detection.

Actions

What happens when a device fails, and when: notify the user, mark it noncompliant after a grace period.

Assignment

The groups it applies to, and the exclusions. Every policy needs a documented exclusion group.

Set the tenant wide default for devices with no policy assigned. Left as compliant, a device outside every policy quietly passes Conditional Access.

The loop that enforces it

01

Evaluate

Intune checks the device against every assigned policy and records a state.

02

Report

That state is written onto the device object in Entra ID.

03

Gate

Conditional Access requires a compliant device for the resources you nominate.

04

Remediate

The user is notified, given a grace period, and told what to fix in Company Portal.

A defensible starting set

RULE	WINDOWS	APPLE	ANDROID
Storage encryption	BitLocker	FileVault, device encryption	Encrypted storage
Minimum version	Supported builds only	Current major, one back	Current major, one back
Password or PIN	Required	Required	Required
Integrity signal	Secure Boot and Defender	Jailbreak detection	Play Integrity

Three patterns to start with

PATTERN	REQUIRES	PROTECTS
Require a compliant device	An Intune compliance state	Email and files from unmanaged machines
Require an approved app	An app protection policy	Work data on personal phones
Block legacy authentication	Modern authentication clients only	The oldest and cheapest attack path

Rolling out access controls safely

Start every policy in report only mode and read the impact before you enable it.

Exclude an emergency access account with stored, monitored credentials from every policy.

Give compliance policies a grace period before they mark a device noncompliant.

Pilot on one ring, then widen. Enforcing everywhere on day one produces an outage.

Compliance, then a gate

01

One policy

Encryption plus a minimum operating system version, assigned to your pilot ring.

02

Set the actions

Notify at day zero, then mark noncompliant after a grace period.

03

Break it

Fail the policy deliberately and read what your test user sees.

04

Report only

Require a compliant device, in report only mode, and read the impact.

Done early? Add the emergency access exclusion to your policy and prove the exclusion works.

Module 06 in short

A compliance policy is rules, actions, and assignment. All three need deciding.

Intune records the state, Entra ID carries it, Conditional Access acts on it.

Report only mode and an emergency access exclusion are not optional.

Set the tenant default for unassigned devices, or they pass your gates silently.

07

Troubleshooting

Where to look, in order

STEP	WHERE	ANSWERS
1	Intune, Troubleshooting and support	Licensed, in scope, under the device limit?
2	Entra ID sign-in logs	Did Conditional Access block the attempt?
3	Enrollment restrictions	Is the platform, version, or ownership blocked?
4	Event log on the device	What did the management client actually report?
5	Diagnostics export	The full picture from the device for an escalation

Failures you will see · identity

No licence on the user, or one assigned moments ago that is not yet effective.

The user sits outside the device management scope, so joining never triggers enrollment.

The device limit is reached, because three retired devices still count against it.

An enrollment restriction is blocking a personally owned device or an old version.

Failures you will see · deployment

The profile is not assigned yet, because the rule-based group has not evaluated.

The status page timed out on a large blocking application over a slow link.

An expired Apple push certificate has taken every Apple device offline at once.

Hybrid join failed on the connector, the organizational unit, or network line of sight.

A device will not enroll

01

Is it registered?

Check the Autopilot device list by serial number. No record means no profile.

02

Is a profile assigned?

Confirm group membership first, then the profile status on the device record.

03

Can the user enroll?

Licence, management scope, device limit, and restrictions, in that order.

04

What did the client say?

The event log and diagnostics on the device. Read the error, not the screen.

Worst enrollment story

What broke, how long did it take to find, and what would you check first now?

Module 07 in short

Work service, then identity, then device. Most tickets end at the first two.

Licences, management scope, device limits, and restrictions cause most identity failures.

Group evaluation delay is the usual reason a profile looks unassigned.

Read the reported error rather than the screen the user is describing.

08

Features worth taking home

What enrollment buys you

Enrollment is the groundwork. What it buys you is a service that can repair a laptop you have never touched, grant administrator rights for ninety seconds and take them back, answer a question about ten thousand devices in one query, remove company data from a personal phone without touching the rest of it, and tell you which application is making your fleet slow. This block is a tour of the parts worth showing your own team.

Control on a phone you do not own

What you control

Encryption of work data inside the app, a required PIN to open Outlook or Teams, limits on copying work content into personal apps, blocking saves to personal storage, and a minimum app or operating system version.

What you do not

The rest of the phone. No enrollment, no inventory of personal apps, no location, and no ability to wipe anything that is not company data.

Removing company data

A leaver keeps their phone and their photos

You request a selective wipe for that user and app

Work mail, files, and the account disappear from Outlook

Nothing personal is touched, and the phone was never enrolled

Remote Help

What it does

Attended remote assistance with both identities verified by Entra ID, the ability to approve administrator prompts, and a record of the session. No inbound firewall rules.

Why it lands

The helper identity is proven to the user and the session is auditable, which is a very different conversation from a third party tool with a shared password.

Privilege management

What it does

A standard user runs one approved application with elevated rights, by rule or by request, and the elevation is logged. Local administrator rights stop being a permanent grant.

Why it lands

It removes the standing administrator account that every audit finding mentions, without the ticket queue everyone fears.

Device query

Ask a question of one device, or of the whole fleet

Answers in seconds, with no report request and no script

Which machines still have that application installed?

Which have less than 10 GB free before the update?

Remediations

What it does

A detection script and a fix script, run on a schedule, reporting how many devices were found broken and how many were repaired.

Where to start

Something small and irritating: a service that stops, a setting users switch back, a folder that fills up. Prove the pattern before you automate anything important.

Endpoint Analytics

Start-up score

How long your fleet takes to become usable, by model. A clear argument for hardware replacement.

Application reliability

Which applications crash, on which builds, on how many devices.

Anomaly detection

Early warning that one update or driver has begun to hurt a particular hardware model.

Certificates from the cloud

What it does

Issues and manages device and user certificates from a Microsoft hosted certificate authority, with no on-premises server, no connector, and no local certificate service to keep alive.

Why it lands

Wireless and network certificates are the last common reason a cloud managed device still needs an on-premises dependency.

Apps without packaging

Enterprise app catalog

Prepackaged, Microsoft maintained applications with updates handled for you.

Package manager and store apps

Point at a package name and let the device fetch and install it.

What is left

Your own line of business installers, which is a much shorter list than it used to be.

Updates that manage themselves

Update rings and policies

A deferral, a deadline, and a grace period per ring, with driver and firmware policies alongside, and feature updates pinned to a version you chose.

Managed updates

Microsoft runs the rings, watches the signals, and pauses a rollout that starts breaking devices.

Copilot in Intune

Explains what a policy actually does, in plain language

Summarises why one device is not compliant

Drafts a device query you would otherwise look up

Better at reading your tenant than at changing it

Requires a Microsoft 365 Copilot license for each admin who uses it

Kiosks, counters, and displays

Windows kiosk

A single app or a restricted desktop, deployed with no user signing in at all.

Android dedicated

Locked to one app or a small set. Well suited to shared field devices.

Shared iPads

Shared mode with per-user data, for libraries and training rooms.

Module 08 in short

App protection controls company data on a phone you do not own or manage.

A selective wipe removes work mail and files and leaves everything personal alone.

Remote Help and privilege management replace standing administrator rights.

Device query and remediations turn recurring tickets into numbers that fall.

Rollout checklist

- 01 Licences assigned and verified on a test user
- 02 Management scope, restrictions, and branding configured
- 03 Groups and naming conventions agreed and created
- 04 Enrollment method chosen per platform and documented
- 05 One device deployed end to end, setup screen to desktop
- 06 Compliance in report only, then enforced ring by ring

Best practices worth adopting

Name things once, deliberately: groups, profiles, group tags, and device names.

Ring your deployments, pilot then early then broad, and never assign to all devices first.

Keep an exclusion group on every assignment and document who may be added to it.

Change one thing at a time, and redeploy a real device to prove it.

Track certificate and token expiry on a shared calendar rather than in memory.

Your first ninety days

Days 1 to 30

Tenant preparation, naming, rings, and one Autopilot device deployed end to end in a test tenant.

Days 31 to 60

A real pilot group on real hardware, compliance in report only mode, and your first boot time measured.

Days 61 to 90

Widen one ring at a time, enforce compliance, and retire the first thing Intune has replaced.

Where to go next

TOPIC	SOURCE
Enrollment methods by platform	Microsoft Learn, Intune device enrollment
Autopilot and device preparation	Microsoft Learn, Windows Autopilot
Apple Business Manager and enrollment	Apple Business Manager user guide
Android Enterprise enrollment	Microsoft Learn, Android enrollment
Compliance and Conditional Access	Microsoft Learn, device compliance policies

Questions

Slides, the checklist, and the reference links go out to attendees after the conference.