MICROSOFT 365 · DEVICE MANAGEMENT FIELD NOTES

Intune device management for small business: registered is not managed

> *Your staff sign in to their laptops with a work account, so the machines look protected. Most of them are only registered, not managed, and that one word is the difference between wiping a lost laptop and hoping. Here is the line, and how to cross it without locking anyone out.*

By **Pedro Bandeira** · 3DH Consulting · Updated August 2026 · 11 min read

The last time I opened the device list for a company that had been running Microsoft 365 for a couple of years, the screen told the whole story in a single column. Nearly every laptop showed one word next to its name: registered. One machine, the newest, showed a different word: joined. To the owner the fleet looked uniform and safe. Everyone signed in with a company account,

everyone had their mail and their files, nothing was obviously wrong. But those two words are not decoration. Registered and joined are two different relationships between the company and the machine, and only one of them means the company is actually in control.

I put Microsoft 365 to work inside small companies, and this is one of the most common gaps I find: a firm that believes it manages its laptops because staff log in with work accounts, when in truth the machines are merely known to the tenant, not governed by it. This is a plain guide to what Intune device management for small business actually changes, why the word on that screen matters more than any security product you might buy, and how to close the gap in an order that does not lock your own people out on the day you tighten the rules.

> **THE GAP THAT HIDES IN PLAIN SIGHT**
>
> A device that is only registered gives you identity and visibility. It does not give you a remote wipe, an enforced encryption key you hold, a compliance verdict, or a single policy you can push. If a registered laptop is lost tomorrow, you cannot reach into it. You can disable the person's account, which matters, but the data already on that disk is a question of whether it was encrypted by luck, not by rule. Managed is the word that turns luck into control.

Registered is identity. Managed is control.

Microsoft draws a clear line here, and it is worth learning because the whole thing turns on it. A Microsoft Entra registered device is typically a personal machine that a person uses for work. Registration gives the tenant an identity for the device and lets it take part in things like single sign-on and Conditional Access. It is the model built for bring-your-own-device: the company gets to know the machine and can gate access through it, but it does not own or run the operating system. A Microsoft Entra joined device is the organization-owned model, the one designed to be run through a mobile device management service such as Microsoft Intune.

The sequence in Microsoft's own documentation makes the distinction concrete. Registration is only the first step. In Microsoft's words, once device registration completes, the process continues with MDM enrollment. Registration writes a device object into your directory. Enrollment is the separate act that hands the machine a set of rules and hands you the levers. A firm that stopped

after step one has a directory full of device names and none of the reach those names imply. The list looks like a managed fleet. It is a guest list.

> **WHAT EACH RELATIONSHIP ACTUALLY GIVES YOU**
>
> Read the middle column as the one that empties bank accounts and the right column as the one that stops it.

CAPABILITY	REGISTERED ONLY	MANAGED (ENTRA JOINED, INTUNE ENROLLED)
Device identity and SSO	Yes	Yes
Remote wipe of company data	No	Yes
Encryption you can prove, key you hold	Not enforced	BitLocker, key escrowed to the tenant
Compliance verdict for Conditional Access	None	Reported to Entra, usable as a gate
Push a policy to the machine	No	Yes, one policy to the whole group

The unmanaged machine is where your keys leak

This is not a theoretical tidiness argument. The device you do not manage is measurably the one that leaks your credentials. Verizon's 2025 Data Breach Investigations Report examined the machines whose logins turned up in the logs of information-stealing malware and found company credentials sitting on 46% of the unmanaged devices it looked at, against 30% of the managed ones. A device outside your control is roughly half again as likely to be quietly handing your working passwords to whoever runs the malware. The same report keeps stolen credentials at the front of the queue as the way attackers get in, which means the leaking device is not a footnote to the breach. It is the on-ramp.

Put the two facts next to each other. Most small companies I see run a fleet that is mostly unmanaged in the technical sense, because it was registered and never enrolled. And unmanaged is the category where the keys leak. The gap on that device list is not a paperwork problem. It is the exact surface the current wave of credential theft is built to exploit, left open by a firm that thought it had already closed it.

The four things managing a device actually buys you

Strip away the jargon and enrollment buys a small company four concrete abilities, each of which answers a real bad day. None of them requires a new product if you are on Microsoft 365 Business Premium, which already carries Microsoft Intune Plan 1. The work is switching them on, in order, and proving each one works before you rely on it.

A machine you can wipe

Enroll a laptop and you can clear the company data from it remotely when it walks out the door with a leaver or a thief. Intune calls the strongest form of this retire, and Microsoft describes it plainly: retiring a device removes it from management and removes all company data from it. On a merely registered machine that option does not exist. You can kill the account, and you should, but the files already on the disk stay on the disk. Wipe is the difference between a lost laptop being an inconvenience and being a disclosure.

A disk nobody can read, with a key you hold

Enrollment lets you require and prove encryption instead of hoping for it. When you deploy it properly, Intune turns on BitLocker and stores the recovery key in your tenant automatically the moment the disk encrypts. The company holds the key, not the employee on a sticky note. That matters twice over: a lost machine is a brick to whoever finds it, and when a firmware update trips a recovery prompt in the middle of an ordinary Tuesday, the forty-eight digit key is one click away in your tenant rather than a lost day and a support ticket. Encryption without escrow is how firms lock themselves out of their own machines. The escrow is the whole point.

A verdict you can gate on

An enrolled device reports a compliance status, and that status becomes something you can enforce. A Microsoft Intune compliance policy is a set of rules a managed device must meet, minimum operating system, disk encryption on, not jailbroken, and the device reports back whether it passes. Feed that verdict into Conditional Access and you can insist that only a machine you vouch for reaches your mail and files. A registered-only device has no verdict to give. It is a name with no report card.

An account that cannot promote itself

The last plank is not glamorous and it is one of the most effective. A managed machine can be built so the everyday account is a standard user rather than a local administrator, which means a piece of malware that lands in that session cannot quietly elevate itself and take the whole device. The one local admin account that still has to exist is handled by Windows LAPS, which rotates that password and stores it in your tenant, so there is no shared admin password on a wiki that every former employee still remembers. Standard-user-by-default turns a single unlucky click into a contained event instead of a company-wide one.

The trap nobody mentions: compliance is off by default

Here is the part that catches careful firms out, the one worth the price of the whole article. Enrolling the devices is necessary, and it is not sufficient. Intune ships with a tenant-wide switch called "Mark devices with no compliance policy assigned as," and its default value is Compliant. In Microsoft's own words, at that default "this security feature is off." A device that has been enrolled but never handed an actual compliance policy is reported to the rest of your tenant as compliant, which is to say as trustworthy, which is to say your Conditional Access gate waves it straight through.

So a firm can enroll every laptop, feel finished, and still be running a fleet that Conditional Access treats as clean because no one flipped that setting to "Not compliant" and no one wrote the policy that actually checks anything. The lights are green because nobody is grading. Closing the gap means three moves, not one: enroll the device, assign it a real compliance policy, and set the tenant to treat an ungoverned device as noncompliant. Miss the third and the first two are a stage set.

> **THE ORDER THAT DOES NOT LOCK OUT YOUR PEOPLE**
>
> Enroll every device first. Then assign compliance policies and set the tenant default to Not compliant. Only then turn on the Conditional Access rule that requires a compliant device. Flip that last rule while machines are still unenrolled and you will lock out your own staff on a Monday morning. Every angry-helpdesk security rollout I have seen turned the final rule on first. Lay the planks, then stand on the floor.

How to check your own fleet in ten minutes

You do not need a consultant to find out where you stand. You need the admin account and ten minutes. Sign in to the Microsoft Entra admin center, open Devices, and look at the list of your machines with the Join type and the managed columns visible. Count them into two piles. The Microsoft Entra joined and Intune-managed machines are the ones you actually control. Everything sitting at Microsoft Entra registered is a machine you can see but not reach. If the second pile is most of your laptops, you have found the single highest-value security project in the company, and it costs configuration time rather than new licences.

- **Open the device list and read the join type.**
  Microsoft Entra admin center, Devices, All devices. Registered is visibility. Joined is control. Count both.
- **Check who is enrolled in Intune.**
  A device can be joined and still not carry policy. The managed column tells you which machines are actually taking instructions.
- **Confirm the compliance setting is on.**
  Endpoint security, Device compliance, Compliance policy settings. If "Mark devices with no compliance policy assigned as" reads Compliant, your gate is not grading anyone.
- **Prove BitLocker escrow on one machine.**
  Encrypt, then confirm the recovery key is visible in the tenant before you trust it. An unproven escrow is a guess.
- **Enroll the fleet before you require it.**

Get every machine to managed and compliant, then, and only then, switch on require-compliant-device in Conditional Access.

What managing the fleet buys you, scenario by scenario

THE LOST LAPTOP

- A machine is left in a taxi or lifted from a bag
- Managed: remote wipe clears the company data on next contact
- Managed: BitLocker makes the disk unreadable, key held by you
- Registered only: you disable the account and hope the disk was encrypted

THE LEAVER

- Someone exits, on good terms or bad
- One action disables their identity across every service
- Managed: the device is retired and its company data removed
- Managed: LAPS means no shared admin password walks out with them

THE INFOSTEALER

- Malware lands on a machine and harvests saved logins
- Standard-user default denies it the rights to take the machine
- Managed devices leak credentials far less often than unmanaged
- Compliance gate blocks a failing device from reaching your mail

THE GREEN LIGHT THAT LIES

- Every device is enrolled, the dashboard looks clean
- But the tenant treats ungoverned devices as compliant
- Conditional Access waves through machines nobody graded
- Fixed by one setting and one real policy, not more software

The same managed floor is what everything above it stands on. You cannot sensibly govern what your staff feed an AI tool if you do not first control which devices your people are logged in on, which is why device management is the groundwork under our EU AI Act readiness work rather than a separate project. And it is the same make-it-real-before-you-build discipline behind our KSeF e-invoicing readiness work: get the boring foundation true, then put weight on it. Foundations first is never the exciting answer. It is the one that holds when something goes wrong.

PEDRO'S TAKE

The companies that get hurt are almost never the ones without a device policy budget. They are the ones who read a directory full of device names and believed the fleet was managed because the names were there. Registered is a guest list. Managed is a lock you hold the key to. If you are on Business Premium you already own Intune, so the work is enrollment and three settings, not a purchase. Open the device list this week and count the two piles. The one word next to each machine is telling you whether, on the worst day, you get to act or only to watch.

Frequently asked questions

Our staff sign in with work accounts. Isn't that enough?

Signing in with a work account registers the device, which gives you identity and lets Conditional Access see it. It does not enroll the device, which is the separate step that gives you remote wipe, enforced encryption with an escrowed key, a compliance verdict, and the ability to push a policy. Microsoft's own documentation treats registration and enrollment as two stages, and most firms complete only the first. The login proves who is at the keyboard. It does not put you in control of the machine.

We are too small to need device management, aren't we?

Size is not the variable that decides this, exposure is. A ten-person firm and a two-hundred-person firm lose the same way: a laptop leaves the building, or an infostealer lands on an unmanaged machine and ships the saved passwords out. The Verizon data is blunt about unmanaged devices being where credentials leak, and automated attacks do not check your headcount before trying a working password. Small firms are hit precisely because they assumed they were beneath notice and left the fleet ungoverned.

Do we need to buy Intune, or new software?

Usually not. Microsoft 365 Business Premium already includes Microsoft Intune Plan 1 and Microsoft Entra ID P1, the device and identity tools this article describes. The task is

configuration, not procurement: enroll the machines, write the compliance policies, and turn on the settings that make them count. The common exception is a firm on a lighter plan such as Business Standard, where the fix is a plan change rather than a separate device-management product bolted on the side.

Not sure how many of your laptops are actually managed?

That is the first thing our device posture review answers. We read your Microsoft Entra device list, count what is registered against what is truly managed, enroll the gap, prove BitLocker escrow before you rely on it, and hand you the enrollment order that gets the whole fleet to compliant without locking anyone out. It uses the licences you already pay for.

Book a device posture call

This is one field note from the weekly edition.

Every Friday I send the week's signals for European SMBs, the rule changes, the Microsoft moves, the traps, in one short email. No hype. **Subscribe on the Pulse page →**

Last updated August 2026. This article is for information only and is not security or legal advice. Key sources: Microsoft Learn documentation on Microsoft Entra device identity and device registration, on Microsoft Intune device compliance policies and Conditional Access, on BitLocker deployment with Intune, and on Windows LAPS (learn.microsoft.com), and the Verizon 2025 Data Breach Investigations Report on managed versus unmanaged devices in infostealer logs (verizon.com).

Not sure where your Microsoft AI actually stands? Take the 10-point readiness check.