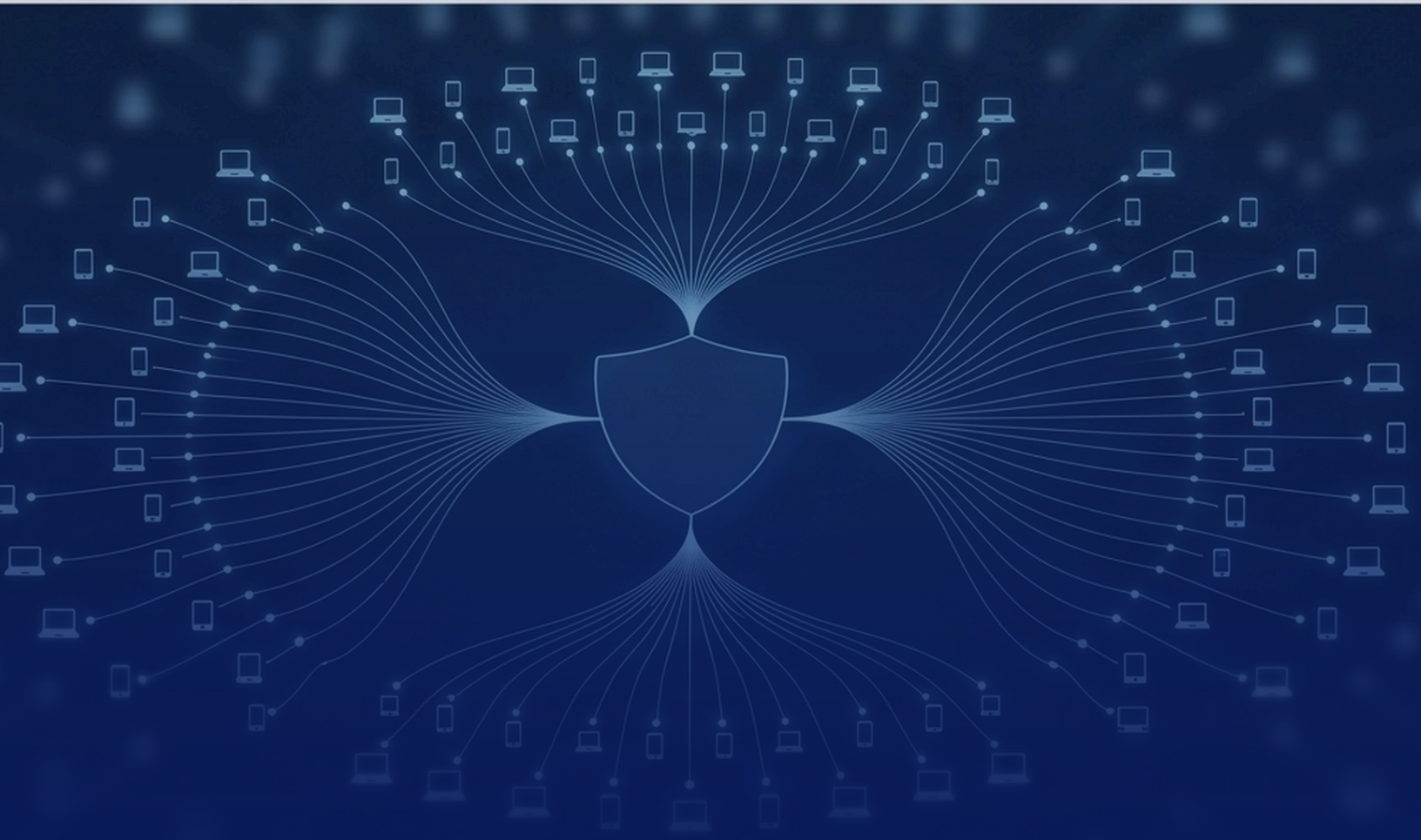

A PLANNING GUIDE FOR IT LEADERS

SCCM to Intune: A Migration Planning Guide

How to move from Configuration Manager to cloud-native management without wiping devices, re-enrolling users by hand, or losing what already works.

LUMEPLEX
INTELLIGENT IT CONSULTING

Lumeplex · Intelligent IT Consulting
lumeplex.com · 2026 edition

EXECUTIVE SUMMARY

Most migrations hurt because they start with configuration instead of a plan

Configuration Manager (SCCM, MECM, ConfigMgr — the same product under three names) has run Windows fleets reliably for two decades. It is also built for a world where devices lived on the corporate network. Microsoft's investment, and every new capability, now lands in Intune. The question for most organizations is no longer *whether* to move, but *how* to do it without breaking the things Configuration Manager quietly does well.

5
planning steps that decide whether the migration is smooth or painful

7
workloads that move, one at a time, through co-management

0
devices that need to be wiped and rebuilt if the plan is right

This guide is written for the IT leader who has been asked "when are we getting off SCCM?" and wants a credible answer. It explains what actually changes and what doesn't, the migration models available, a five-step planning method, how to move each workload, how to design the pilot, and the risks that derail projects. It is deliberately practical: every section ends with something you can do this week.

What's inside

> **The single most important idea in this guide:** co-management lets Configuration Manager and Intune manage the same device at the same time. You move responsibilities across one workload at a time, on your schedule, and you can move any of them back. Nothing about this has to be a big bang.

CONTEXT

Why move, and why now

Configuration Manager is not broken. It images machines, deploys applications, patches Windows and reports on all of it with a depth that Intune is still catching up to in places. If everything you manage sits on a corporate network, in an office, on Windows, you could keep running it for years.

Almost nobody's environment looks like that any more. Three pressures push organizations towards Intune, and they tend to arrive together.

Devices are off the network. Configuration Manager reaches a laptop when it is on the LAN or VPN. A cloud management gateway extends that, at a cost, but the design assumption remains that the network is the control channel. Intune assumes the internet is. For a hybrid workforce, the difference shows up as patch compliance numbers you can't defend and remote staff you can't help.

The estate isn't just Windows. Macs, iPhones, iPads and Android devices are corporate endpoints now. Configuration Manager was never meant to manage them; Intune manages all of them from one console, with the same compliance and access rules.

Security has moved to identity and device health. Conditional Access, Defender for Endpoint integration, device compliance as a condition of reaching email — these are Intune-native features. Configuration Manager can feed

compliance into them only through co-management. If your security roadmap includes Zero Trust, it runs through Intune.

Add to this the practical costs that accumulate around an on-premises management platform: site servers and SQL to patch and back up, distribution points in every office, a cloud management gateway subscription, the specialist skills to keep it all healthy, and the fact that Microsoft's new features — Autopatch, Endpoint Privilege Management, Remote Help, Copilot for device management — ship to Intune first or only.

None of this means you must move everything tomorrow. It does mean the direction is settled, and the organizations that plan the move deliberately get to choose the pace. The ones that don't plan tend to be forced into it by a hardware refresh, an audit finding or a security incident, which is the worst time to learn a new platform.

> **Do this week:** count the devices that connected to Configuration Manager in the last 30 days, and the devices Entra ID has seen sign in over the same period. The gap between those two numbers is the size of your unmanaged-endpoint problem, and it is the strongest argument you will find for the project.

EXPECTATIONS

What changes and what doesn't

The most common mistake is to treat the migration as a lift-and-shift: export every package, task sequence and collection, and recreate it in Intune. That approach fails because the two products manage devices differently. Intune is declarative — you describe the state you want and the device converges on it — while Configuration Manager is procedural: you tell it exactly what to run, in what order, on which collection.

Area	In Configuration Manager	In Intune
Building a device	Task sequence applies an image, drivers, apps and settings in the office	Autopilot: the OEM's image, plus Intune policy and apps applied on first sign-in, anywhere
Applications	Packages and applications with detection rules, deployed to collections	Win32 apps (the same installers, repackaged as .intunewin) and Microsoft Store apps, assigned to Entra groups
Settings	Group Policy, plus configuration baselines	Settings Catalog and configuration profiles; Group Policy analyzed and migrated where it still matters
Windows updates	Software update groups and deployment packages from WSUS	Update rings, feature-update policies, and Windows Autopatch — from Microsoft, not from your server

Compliance	Reporting on what's installed	Compliance policies that feed Conditional Access — non-compliant devices lose access
Targeting	Collections built on inventory queries	Entra ID groups (dynamic and assigned) and filters
Reporting	Very deep, SQL-based, customizable	Built-in reports plus Intune data warehouse and Log Analytics; less depth, more current
Servers	Site server, SQL, distribution points, CMG	None. Microsoft runs the service

What doesn't change

- **Your applications.** The same installers work; they are packaged differently and detection logic is rewritten, but you do not need new software.
- **Your security requirements.** Encryption, patch cadence, admin rights, antivirus — the policies carry over; only the enforcement mechanism moves.
- **Your users' devices.** With co-management, existing Windows 10/11 devices enroll in Intune in place. No wipe, no re-image, no hand-re-enrollment.
- **Your team.** Configuration Manager administrators become Intune administrators. The concepts transfer; the console and the vocabulary are new.

> **Do this week:** list your task sequences and count the steps in each. Anything that exists only to work around imaging — driver injection, disk layout, domain join — disappears with Autopilot. What remains is the list of settings and apps you actually need to recreate.

APPROACH

Three migration models, and which one to choose

1. Co-management (recommended for almost everyone)

Existing devices stay in Configuration Manager and are also enrolled in Intune. Seven workloads — compliance policies, device configuration, Endpoint Protection, resource access, Office Click-to-Run apps, client apps and Windows Update policies — are switched from Configuration Manager to Intune one at a time, using a pilot collection first. Any workload can be switched back. When every workload is on Intune, the Configuration Manager client is removed and the device is fully cloud-managed. New devices are built with Autopilot from day one and never touch Configuration Manager at all.

Choose it when you have a working Configuration Manager environment, more than a couple of hundred Windows devices, and a business that cannot tolerate disruption. This is the model this guide

assumes.

2. Side-by-side (clean cut per device)

Intune is built out fully in parallel. Devices move one at a time — typically when they are refreshed or re-imaged — by being reset and provisioned with Autopilot. Old devices stay on Configuration Manager until they leave the estate.

Choose it when your Configuration Manager environment is unhealthy or heavily customized, a hardware refresh is already scheduled, or the fleet is small enough that a reset per device is acceptable. Slower for the estate as a whole, but every migrated device is clean.

3. Big bang

All devices are enrolled in Intune and Configuration Manager is switched off over a weekend. We list it for completeness. It works only for very small, very simple environments, and it forfeits the main advantage of co-management: the ability to find out what breaks with ten devices instead of a thousand.

Factor	Co-management	Side-by-side	Big bang
Disruption to users	Minimal — in-place, staged	One reset per device	High
Time to first value	Weeks (first workload)	Weeks (first Autopilot devices)	Days, if nothing breaks
Time to retire SCCM	3–9 months	Tied to hardware refresh cycle	Immediate
Ability to roll back	Per workload, any time	Per device, with a rebuild	Effectively none
Best for	Most organizations with 200+ devices	Refresh-driven or unhealthy SCCM	Under ~50 devices, simple needs

> **Do this week:** check whether your devices are hybrid-joined to Entra ID and whether the Configuration Manager client is current. Both are prerequisites for co-management and both are frequently half-done in environments that "already set that up years ago".

METHOD

The five-step planning method

A good plan is the difference between a migration your users don't notice and one they talk about for years. These five steps take two to four weeks and produce a plan your team can execute — or hand to a partner with confidence.

1. **Assess the current state.** Configuration Manager health (site status, client versions, SQL, boundaries), Active Directory and Entra ID hybrid join status, Intune licensing and tenant configuration, Conditional Access, network egress to Microsoft endpoints, and the device fleet by model, OS version and location. This step routinely uncovers the surprises — the unlicensed users, the devices joined to the wrong domain, the proxy that blocks enrollment.

2. **Catalogue the use cases and the inventory.** Not "what does SCCM do" but "what do we need devices to do". Build the list: onboard a new starter, replace a broken laptop, deploy an application, patch a zero-day, retire a leaver's device, prove compliance to an auditor. For each, note who is involved and how long it takes today. Alongside it, inventory applications (with usage data — most estates carry dozens of apps nobody has opened in a year), Group Policy objects, and every task sequence step.

3. **Run the gap analysis.** For every use case and every setting, decide: *Intune-native* (Settings Catalog, compliance, Win32 app), *needs redesign* (a printer-mapping script becomes Universal Print; a drive-mapping GPO becomes a OneDrive/SharePoint sync), *retire* (workarounds for imaging, settings nobody remembers the reason for), or *keep on SCCM for now* (a rare on-premises-only requirement). Group Policy Analytics in Intune does the first pass on GPOs automatically.

4. **Draft the migration plan.** The target design (naming, groups, policy structure, update rings, Autopilot profiles), the co-management workload order, the pilot groups, the rollout waves, the communications plan, and the decommission criteria for Configuration Manager. Include the things that are easy to forget: how the service desk will support a co-managed device, how you'll handle the devices that never check in, and what "done" means for each workload.

5. **Workshop and finalize the roadmap.** Walk the plan through with the people who will live with it: IT operations, the service desk, security, and a representative from the business side. Adjust, assign owners and dates, and agree the go/no-go criteria for each wave. The output is a roadmap with a first-workload date inside 30 days.

> **Why the catalogue matters more than the tool.** Every troubled migration we have reviewed skipped step 2. Teams recreated Configuration Manager in Intune, feature for feature, and then discovered that half of what they built was for use cases that no longer existed and the other half missed the things users actually did.

EXECUTION

Moving the workloads, one at a time

Co-management exposes seven workload sliders. The order below is the one we recommend for most organizations: each move is low-risk on its own and prepares the ground for the next.

1 Compliance policies

Move this first. Intune evaluates encryption, OS version, Defender status and password rules, and reports each device as compliant or not. On its own this changes nothing for users; it gives you the data. Later, Conditional Access will use it. **Watch for:** devices that are non-compliant for boring reasons (an old OS build, BitLocker never turned on) — fix those before you ever enforce.

2 Windows Update policies

Retire WSUS. Update rings (pilot, early, broad) with deferral and deadline settings, plus feature-update policies to hold a Windows version until you're ready. Windows Autopatch automates the rings if you'd rather not manage them. **Watch for:** devices that were pointed at WSUS by Group Policy — the GPO must be removed or the device stays split between two update sources. Set Windows to "scan against Windows Update" explicitly.

3 Endpoint Protection

Defender antivirus, firewall, BitLocker and attack-surface-reduction settings move into Intune's endpoint security policies. If you use Defender for Endpoint, its security-settings management can apply the same policies to devices that aren't even enrolled. **Watch for:** BitLocker recovery keys — confirm they escrow to Entra ID before you move the policy, and test recovery on a real device.

4 Device configuration

The largest workload. Run Group Policy Analytics against your GPOs to see which settings have Intune equivalents (most do), build them in the Settings Catalog, and assign to the pilot group. Keep the GPOs in place during co-management — when both apply, the Intune setting wins by default, so conflicts surface early and safely. **Watch for:** logon scripts and drive mappings, which need redesign rather than migration; and settings nobody can explain, which you should retire, not port.

EXECUTION

Moving the workloads, continued

5 Resource access

Certificates, VPN and Wi-Fi profiles. Intune delivers these through SCEP or PKCS connectors to your certificate authority, or through Microsoft Cloud PKI if you would rather not run one. **Watch for:** the on-premises CA that has never been used outside the LAN; test certificate issuance to a device on a home network before you commit.

6 Office Click-to-Run apps

Microsoft 365 Apps installation and update channel move to Intune. Small on its own, but it removes one more dependency on Configuration Manager's content distribution. **Watch for:** update channel mismatches between what Configuration Manager was enforcing and what Intune assigns, which produce unexpected version changes.

7 Client apps

Usually last, because it is the most work. Each application you decided to keep in the catalogue step is repackaged as a Win32 app (the .intunewin format), given detection rules and requirements, and assigned to groups — as required, available in the Company Portal, or uninstall. Microsoft Store apps and the Enterprise App Catalog cover the common ones without packaging. When this workload moves, Configuration Manager and Intune apps can coexist on the same device; you migrate app by app. **Watch for:** apps that depend on being on the network for licensing or activation, and installers that assume a logged-on user.

New devices: Autopilot from day one

While existing devices move through co-management, every new or re-imaged device should be built with Windows Autopilot and never see Configuration Manager. Register devices with your hardware supplier at the point of purchase, define an Autopilot profile (user-driven, Entra-joined for most; hybrid-joined only if a hard on-premises dependency remains), and use an Enrollment Status Page to make sure required apps and policies land before the user reaches the desktop. This is where the "no imaging bench" benefit arrives, and it is usually the moment stakeholders become believers.

Workload	Typical effort	User-visible?	Rollback
Compliance	Days	No	Slider back

Windows Update	1–2 weeks incl. pilot	Reboot prompts change	Slider back + GPO
Endpoint Protection	1–2 weeks	No	Slider back
Device configuration	2–6 weeks	Occasionally	Slider back; GPO still applies
Resource access	1–2 weeks	No, if tested	Slider back
Office apps	Days	No	Slider back
Client apps	Weeks to months, by app count	Company Portal appears	Per app

ROLLOUT

Designing the pilot and the rollout

The pilot is not a demo. It is where you find the printer that only maps on the LAN, the finance app that checks for a domain, and the laptop model whose firmware breaks Autopilot. Design it to find those things.

Choosing pilot devices and people

- **Every device model** in the estate, not just the newest. Firmware and driver behavior differ by model, and Autopilot registration must be tested per model.
- **Every kind of user:** office-based, fully remote, a traveller, a shared-device user, an executive with an assistant, someone from finance and someone from IT. Aim for 10–25 devices for the first wave.
- **People who will tell you the truth.** The pilot needs honest, prompt feedback more than it needs enthusiasm. Give them a direct channel to the project team and a two-day response promise.

Test each use case end to end

Take the catalogue from the planning phase and run every use case on pilot devices: onboard a new starter with Autopilot from an unopened box, replace a broken laptop, install an app from the Company Portal, patch a device that has been off for a month, wipe and reassign a device, produce a compliance report. Record the time each takes and who touched it. These numbers become your before-and-after story.

Waves and go/no-go

After the pilot, roll out in waves of a size your service desk can support — often 10–15% of the estate per wave, weekly or fortnightly. Each wave gets a go/no-go review against simple criteria: pilot tickets resolved, compliance percentage above target, no open severity-1 issues. Communicate to every wave

twice: a week before ("here is what will change") and the day of ("here is what you'll see, here is how to get help").

Equip the service desk before the first wave

Front-line support needs to know how to check a device's co-management state, where compliance is reported, what a Company Portal is, and how to escalate. A one-hour session and a one-page cheat sheet prevent the most common early complaint: "IT didn't know about it either."

> **Do this week:** write down the six to ten use cases you will test in the pilot, and the person who will sign each one off. If you cannot name the person, the use case is not ready to test.

RISK

Risks that derail migrations, and how to avoid them

Risk	What it looks like	How to avoid it
Recreating SCCM in Intune	Hundreds of policies and packages ported feature-for-feature; months of effort; a design nobody can explain	Catalogue use cases first. Port what is needed, redesign what should change, retire the rest.
Hybrid join half-done	Devices that show in Entra ID as pending, enrollment failures, Conditional Access blocking the wrong people	Verify Entra Connect device write-back and hybrid join for every OU in the assessment, before touching workloads.
Two update sources	Devices patched by both WSUS and Windows Update, or by neither; reboots at random times	Remove WSUS GPOs at the same moment the update workload moves. Use a pilot ring and deadlines with grace periods.
Conditional Access surprises	The CEO locked out of email on a Monday morning because a compliance policy tightened	Report-only mode for two weeks, break-glass accounts, staged enforcement, a named person on call for the first days.
Apps that assume the LAN	Licensing servers, mapped drives, printer scripts fail for remote users	Identify in the gap analysis; redesign (Universal Print, SharePoint sync, cloud licensing) before rollout.
Nobody owns the decisions	The project drifts; every setting becomes a debate; SCCM never gets switched off	Assign a single owner with authority to decide, and agree decommission criteria on day one.

Skills gap	The SCCM team is nervous; mistakes in the new console; slow troubleshooting	Train the team during the pilot, document every design decision, and plan a knowledge-transfer session per workload.
Decommissioning too early	A forgotten dependency — a task sequence used once a quarter, a report finance relies on	Run Configuration Manager read-only for 30–60 days after the last workload moves, then remove clients, then retire the site.

How long does it take?

For an organization with 200–1,000 Windows devices and a healthy Configuration Manager environment, planning takes two to four weeks, the first workloads move within a month, and full decommission typically lands three to nine months after the start. The width of that range is almost entirely the application workload: an estate with 30 apps moves quickly; one with 300 takes a rationalization exercise first. Migrations that skip planning do not finish faster — they finish later, after a pause to plan.

READINESS CHECKLIST

Are you ready to start?

- [ ] Every user who will have a managed device holds an Intune license (Business Premium, E3, E5 or an Intune add-on).
- [ ] Configuration Manager is on a current branch and site health is green.
- [ ] Devices are hybrid-joined (or Entra-joined) and show as such in Entra ID.
- [ ] Network egress to Microsoft endpoints is allowed from every site, without SSL inspection on the management traffic.
- [ ] You have a use-case catalogue and an application inventory with usage data.
- [ ] Group Policy Analytics has been run and the results reviewed.
- [ ] Pilot devices cover every hardware model and every kind of user.
- [ ] A single named owner has the authority to make design decisions.
- [ ] Decommission criteria for Configuration Manager are written down.

ABOUT LUMEPLEX

Lumeplex is a Microsoft-focused IT consultancy based in Dallas, Texas. Our team spent more than a decade designing and running endpoint, identity and security environments for large, regulated organizations — including Configuration Manager estates at enterprise scale and their migrations to Intune. We bring the same architecture-led, phased approach to growing businesses.

How we can help

SCCM to Intune Migration Planning. The five-step method in this guide, delivered as a scoped engagement: assessment, use-case catalogue, gap analysis, migration plan and a roadmap workshop with your team. Remote, in two to four weeks.

Migration execution and Intune deployment. Co-management setup, workload moves, Autopilot, application packaging and knowledge transfer — as a project, or run into an ongoing managed service.

Get a free strategy call at lumeplex.com/contact