GPO to Intune Migration Checklist for Australian Businesses

A comprehensive guide for Australian SMBs transitioning from Group Policy to Microsoft Intune

Build for IT Managers, Microsoft 365 Admins and Modern Workplace Engineers

July 2025

Phill McSherry

MIGRATION ESSENTIALS • MICROSOFT INTUNE

GPO to Intune Migration Checklist

Reference Guide • July 2025 Edition

A practical guide for Australian SMBs modernising their endpoint management

This checklist is designed to help IT managers and sysadmins transition from legacy Group Policy Objects (GPOs) to cloud-native policy management through Microsoft Intune.

It breaks the migration process into practical, manageable stages—covering planning, auditing, mapping, testing, execution, and validation.

The goal is to provide a clear, structured reference that reflects real-world priorities, so you can modernise confidently without unnecessary risk or complexity.

"Modern device management isn't just about policy—it's about clarity, security, and scale."

Who Should Use This Checklist?

- SMB IT Managers
- Microsoft 365 Administrators
- System Engineers transitioning from on-prem Active Directory

This guide assumes you already have a Windows domain environment in place and are seeking to modernise using Microsoft Intune and Entra ID.

🧭1. Pre-Migration Planning

Preparing for a Group Policy migration to Microsoft Intune requires more than just flipping switches—it's about rethinking how you manage modern Windows devices. This section helps you lay the groundwork for a successful transition by assessing your current environment, identifying dependencies, and aligning your goals with what cloud-native policy management offers.

A thoughtful pre-migration phase helps avoid missteps, especially in small-to-mid-sized businesses where IT resources are limited and disruption must be minimal. Use this page as your initial guidepost for setting project direction and expectations.

Before migrating policies, it's crucial to build a clear picture of your current environment and understand how it aligns with modern cloud-native management. This section helps you avoid surprises and set a realistic plan based on your current GPO estate.

Checklist:

- **List your management tools:** Identify if you're using on-prem AD, hybrid join, or Entra ID-only. Clarify how Group Policy is currently applied.
- **Define scope of migration:** Decide if this is full cloud transition (Entra-only) or hybrid co-management. Consider user/device numbers, remote work, and compliance needs.
- **Check Intune licensing:** Confirm you have Microsoft 365 Business Premium or Enterprise E3/E5 licenses with Intune and Autopilot.
- **Document device types and OS versions:** Ensure all devices are Windows 10/11 Pro or Enterprise, version 21H2 or later, and Entra Join or hybrid-capable.
- **Flag blockers early:** Note anything that might delay or prevent migration: legacy applications, network dependencies, or strict compliance regimes.
- **Communicate change plan internally:** Get stakeholder buy-in and inform users about possible changes to experience or policy enforcement.

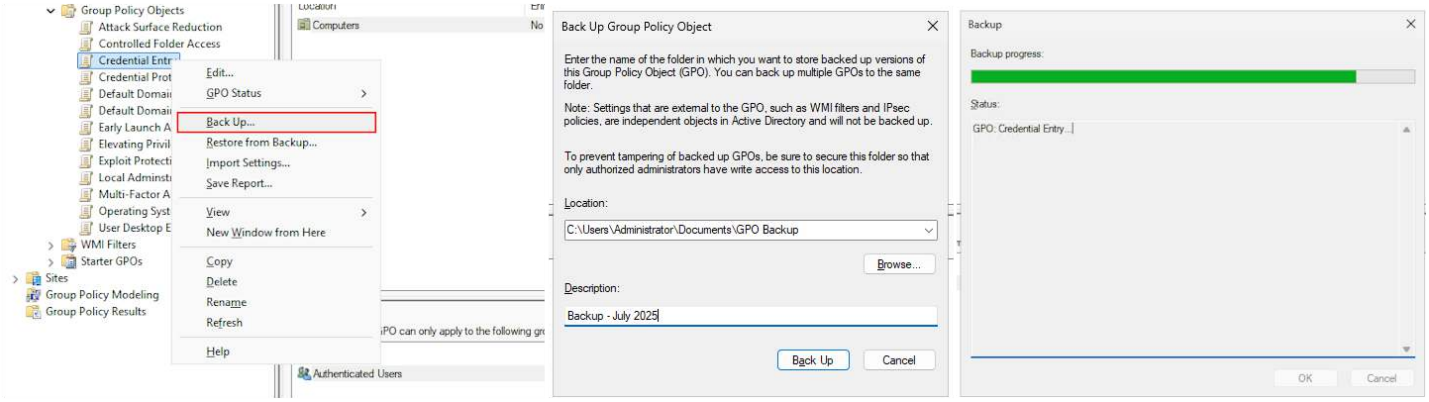
🗂️2. GPO Audit & Grouping

Before migrating anything, run a full audit of your existing Group Policy Objects using built-in tools like Group Policy Management Console (GPMC) or export scripts.

Categorising your policies helps you plan the migration in logical stages and reduce complexity.

Checklist:

- **Export and back up all existing GPOs:** Use GPMC or PowerShell scripts to back up all current Group Policies.
- **Identify duplicate or conflicting policies:** Review policy overlap across GPOs to identify redundant or conflicting settings.
- **Categorise GPOs by use-case:**
    - *Security Baselines:* password policies, firewall, lockout rules
    - *User Experience:* wallpaper, Start menu, taskbar layout
    - *Scripts & Preferences:* logon scripts, mapped drives, scheduled tasks
- **Group GPOs by user/device targeting logic:** Clarify if GPOs are user-based, device-based, or filtered via security group or WMI.
- **Highlight unsupported legacy settings:** Note Internet Explorer policies, control panel restrictions, or legacy templates that have no cloud equivalent.
- **Prioritise what must migrate first:** Start with security or compliance-sensitive policies.



⚙️3. Intune Feature Mapping

Once you've audited your existing GPOs, the next step is mapping each policy to its modern equivalent in Microsoft Intune. This isn't always a direct match—and that's okay. The goal isn't to clone every policy but to modernise how configuration is applied, secured, and maintained in a cloud-first world.

Think of this stage as policy translation: deciding which legacy settings stay, which ones go, and which are reimagined using modern tools like the Settings Catalog, ADMX-backed templates, or scripting. By breaking this into method-based buckets, you create a more sustainable configuration model going forward.

Not all GPO settings have a direct 1:1 match in Intune. This section helps map your policies to the most appropriate Intune configuration method: Settings Catalog, Administrative Templates (ADMX), PowerShell, or Win32 apps.

Checklist:

- **Manually compare your GPO settings with available MDM policies:** Use the Intune Settings Catalog, ADMX-backed policies, and Microsoft Docs to determine coverage.
- **Settings Catalog for most policies:** Modern replacement for traditional ADMX; most new features land here first.
- **ADMX-backed policies for legacy settings:** Useful for more complex or traditional settings like Office or OneDrive controls.
- **PowerShell for complex logic or scripting:** Ideal for scheduled tasks, registry tweaks, or settings without UI equivalents.
- **Win32 apps for complex deployments:** Use the Win32 app model for things like fonts, drivers, MSI deployment, or advanced scripting.
- **Record method used for each GPO item:** Maintain a tracking worksheet with columns for "Old GPO," "Mapped To," "Status," and "Notes."

Sample Worksheet Template:

Old GPO Setting	Intune Equivalent	Method Used	Status	Notes
Prevent access to Control Panel	Settings Catalog → User Configuration	Settings Catalog	Migrated	Used CSP ControlPolicySettings/NoControlPanel
Set Desktop Wallpaper	Settings Catalog → Device Configuration	Settings Catalog	Planned	Needs image URL hosted in public endpoint
Disable command prompt	Not available in Intune	N/A	Skipped	No direct replacement, deemed unnecessary
Map network drive at logon	Use PowerShell script in Intune	PowerShell Script	In Progress	Requires Azure Files or OneDrive Mapping
Configure Windows Defender exclusions	Endpoint Security Baseline	Security Baseline	Migrated	Verified via Compliance Policy Report
Office macro settings	ADMX Templates → Microsoft Office	ADMX	Planned	Cross-check with M365 compliance centre

🧪 4. Pilot & Test Planning

Rolling out new policies across your environment without testing is a recipe for surprises—none of them good. A structured pilot phase gives you space to validate how policies behave in real-world conditions, with a limited user base and clear rollback options.

This stage is your dress rehearsal: it allows you to test compliance, stability, user experience, and app readiness before moving to full production. It's also a key opportunity to build confidence across your organisation, gather feedback, and fine-tune your rollout approach based on real data.

Before going organisation-wide, test your policies in a safe, controlled way. A well-planned pilot phase catches issues early and builds stakeholder confidence.

Checklist:

- **Create a test group in Entra ID:** Use dynamic groups or manually assign test devices and users.
- **Use dedicated Autopilot profiles for testing:** Set up an isolated testing profile to validate OOBE experience and device provisioning.
- **Apply policies gradually:** Test security, user experience, and compliance settings in stages.
- **Use test users for login scenarios:** Validate whether policies apply correctly to real-world user types (admin, standard, roaming profiles).
- **Document issues and feedback:** Track success, failures, error codes, and UX issues for each phase.
- **Run compliance and analytics reports:** Use Intune's built-in reporting and Endpoint Analytics for telemetry.
- **Refine before rollout:** Use pilot results to make changes, tighten configurations, or adjust rollout schedule.

🚀5. Migration Execution

Now that testing is complete and you're confident in your policies, it's time to execute the migration in production. This is the phase where planning pays off—rolling out changes in a controlled, strategic sequence will minimise disruption and ensure business continuity.

You'll need to manage coexistence between legacy GPOs and modern Intune policies carefully to avoid conflicts. You'll also want rollback plans and communication strategies ready, just in case issues arise. Treat this like a phased project rollout, not a big-bang switchover, and document every step along the way for governance and troubleshooting.

This is the step-by-step process of moving away from on-prem GPOs and into modern cloud policy. You'll want a clear sequence, rollback options, and internal documentation to avoid disruption.

Checklist:

- **Start with new devices (greenfield):** Use Autopilot and Intune policies only on new laptops or rebuilds to validate clean deployments.
- **Use device configuration profiles over user policies:** Where possible, apply device settings for consistency and control.
- **Avoid "double policy" conflict:** Do not apply GPO and Intune equivalent simultaneously. Phase out GPO as cloud policy succeeds.
- **Disable GPOs in stages:** Use security filtering or WMI to disable GPOs on migrated devices only.
- **Have rollback options ready:** Export Intune config before changes; back up registry or profile states for critical policies.
- **Log each phase of rollout:** Document when and how policies were applied, and the outcomes.
- **Track support tickets:** Keep a log of user-reported issues tied to policy rollout.

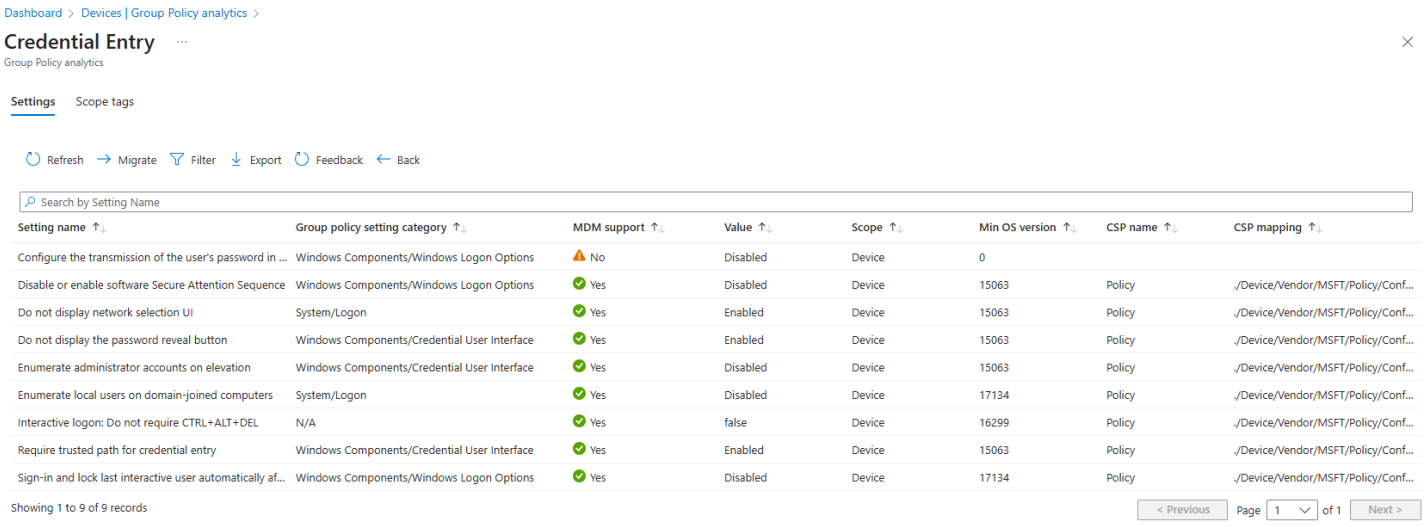
✅6. Post-Migration Validation

You've completed your rollout—now it's time to verify that everything's working as intended. This is where your planning and testing pay off. The goal now is to confirm policies applied successfully, track any drift, and ensure the user experience remains consistent.

Once policies are live in production, you need ways to validate success and monitor behaviour. This is where visibility and analytics make the difference between "done" and "done right."

Checklist:

- **Run Intune Compliance Policy reports:** Confirm devices are applying required settings and are compliant.
- **Monitor Configuration Profile status:** Look for "Succeeded," "Error," or "Pending" states and investigate any failures.
- **Use Endpoint Analytics to spot trends:** Check boot times, policy success rates, app readiness, and user impact.
- **Cross-check against original GPO intentions:** Ensure the new cloud policy matches the old GPO goal—not just the setting.
- **Re-survey test users post-rollout:** Get quick feedback on login times, mapped drives, Start menu layout, and general experience.
- **Review audit logs and security baselines:** Confirm there are no unexpected security drifts after migration.
- **Update your documentation:** Note final config, who owns it, and how it's maintained going forward.



📌 Next Steps

Your GPO-to-Intune migration is a major step toward modernising your device management and security posture. But the work doesn't stop after the last policy applies. Now is the time to ensure your environment remains secure, maintainable, and optimised for growth.

Whether you're still planning or already deep into your migration, Titan Solutions can help with strategic planning, technical implementation, or post-deployment tuning.

Need help planning or executing your GPO-to-Intune migration? Book a free 30-minute strategy session with Titan Solutions to explore how we can assist with planning, implementation, or post-migration review.

🎯 Book your free 30-minute consultation today
bookings.titansolutions.com.au

We're here to help you transition with confidence — whether you're just exploring or ready to go.