Strategic Migration Blueprint: Transitioning from GPO to Microsoft Intune

Version:
0.9 Draft

Author:
daniel.metzger@microsoft.com
Cloud Solution Architect

February 6, 2026

Contents

Strategic Migration Blueprint: Transitioning from Group Policy Objects to Microsoft Intune for Windows 11 Client Devices

Executive Summary

Today's enterprise computing environment requires organizations to reconsider traditional device management approaches. Companies utilizing co-managed solutions – where both Microsoft System Center Configuration Manager (SCCM) and Microsoft Intune administer Windows 11 clients with hybrid Microsoft Entra ID domain membership – now face the need to shift towards cloud-native management models. This document presents a detailed, phased migration strategy intended to assist IT professionals in systematically moving from Group Policy Object (GPO)-based management to exclusive use of Microsoft Intune policy frameworks, ultimately establishing an entirely cloud-managed infrastructure with all Windows 11 client devices natively joined to Entra ID.

The outlined migration framework addresses the technical challenges associated with removing legacy Active Directory dependencies while ensuring continued operational effectiveness and security throughout the transition. It emphasizes utilizing built-in Microsoft tools such as Group Policy Analytics in the Intune administrative console, the Microsoft Security Compliance Toolkit, and Intune's security baseline templates. Additionally, this guide clarifies essential architectural differences between GPO-based and Mobile Device Management (MDM)-based policy enforcement methods, which necessitate their complete separation during the migration process.

Document Scope and Objectives

Primary Objective Migrate from GPO and SCCM co-management to cloud-native Intune-only management for Windows 11	**Identity Transition** Move from hybrid Entra ID joined to cloud-only Entra ID joined device state
Security Posture Implement Microsoft Security Compliance Toolkit baselines via Intune security policies	**Operational Model** Eliminate co-management complexity and establish unified cloud-based device management

Learn about Intune security baselines for Windows devices - Microsoft Intune | Microsoft Learn

Default configuration of Intune's Windows security baselines - Microsoft Intune | Microsoft Learn

Understanding the Current State Architecture and Target End State

Current Environment Characteristics

The present operational environment encompasses Windows 11 client devices administered through a co-management configuration that integrates both Configuration Manager (SCCM) and Microsoft Intune management authorities. These devices maintain hybrid Entra ID-joined status, signifying simultaneous membership in both the on-premises Active Directory domain infrastructure and the cloud-based Entra ID tenant. Configuration settings are currently enforced through traditional Group Policy Objects processed via on-premises domain controller infrastructure, supplemented by selected workload categories that may have been transitioned to Intune management as part of the initial co-management enablement. This dual-management topology, while providing transitional flexibility, introduces inherent policy conflict risks and management complexity that ultimately undermines the security and operational efficiency objectives of modern cloud-native architectures.

Switch co-management workloads - Configuration Manager | Microsoft Learn

Diagnose MDM enrollment failures | Microsoft Learn

Co-management workloads - Configuration Manager | Microsoft Learn

The co-management framework employs a workload delegation approach, allowing organizations to reassign specific management domains – such as Compliance Policies, Windows Update Policies, Resource Access Policies, Endpoint Protection, Device Configuration, Office Click-to-Run Applications, and Client Applications – from Configuration Manager oversight to Intune control. This transition is managed via administrative slider controls within the Configuration Manager console. Typically, all workloads initially remain under Configuration Manager authority, with gradual migration of individual workloads conducted through pilot collection testing prior to full-scale deployment.

Target State Architecture

The overarching strategy aims to establish a fully cloud-native endpoint management solution defined by several key characteristics. Foremost among these is the adoption of exclusive native Entra ID-joined device identities, replacing hybrid Entra ID join status to eliminate reliance on on-premises Active Directory for authentication and policy enforcement. Under this model, Microsoft Intune assumes responsibility for all configuration and security policy management, leveraging cloud-based delivery mechanisms that function independently of corporate network connectivity or direct access to domain controllers. Ultimately, the Configuration Manager (SCCM) client agent is removed from devices, fully retiring co-management architectures and alleviating the complexity associated with dual management systems.

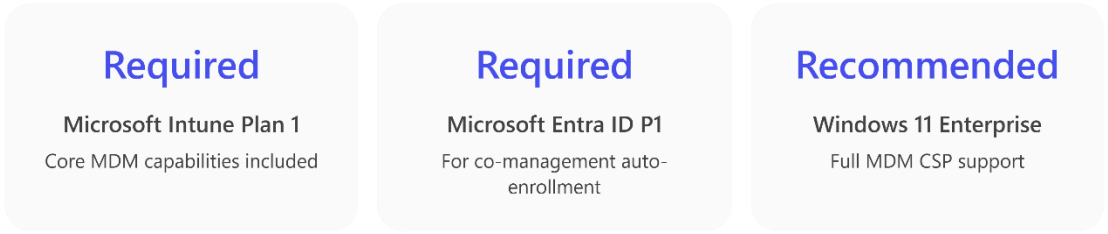
This evolution represents more than a technological migration; it signifies a fundamental shift in enterprise security paradigms. The adoption of a cloud-native model elevates identity to the role

of primary security boundary, superseding traditional dependence on network location. This enables the implementation of advanced conditional access policies that assess a broad spectrum of risk indicators – including user risk profiles, device compliance status, application sensitivity, and geographic context – before authorizing resource access. Achieving a Zero Trust security posture is contingent upon decoupling devices from on-premises domain infrastructure, as hybrid-joined devices perpetuate outdated trust models rooted in network location rather than ongoing verification of identity and device integrity.

Licensing Requirements and Prerequisites

Microsoft Intune Licensing Models

The deployment of Microsoft Intune for comprehensive Windows 11 device management requires appropriate licensing for all users whose devices will be enrolled. Microsoft provides Intune licensing through multiple subscription models, each offering distinct features and pricing structures. Organizations frequently acquire Intune licenses via bundled enterprise agreements rather than standalone subscriptions, as these packages typically deliver greater functionality and cost efficiency.



The Microsoft 365 E3 licensing tier includes Intune Plan 1, which offers essential Mobile Device Management (MDM) and Mobile Application Management (MAM) capabilities suitable for standard enterprise requirements. This tier supports core Intune features such as device enrollment, configuration profile deployment, application management, compliance policy enforcement, and integration with Microsoft Defender for Endpoint to provide basic threat protection. For organizations requiring enhanced security and compliance features, the Microsoft 365 E5 tier builds on Intune Plan 1 with advanced threat analytics, privilege access management, and expanded compliance reporting. From 2026 onward, Microsoft will integrate Intune Suite capabilities into both E3 and E5 subscriptions, broadening feature availability without necessitating separate Intune Suite licenses.

Additional licensing options include the Enterprise Mobility + Security (EMS) E3 and EMS E5 suites, which combine Intune with Microsoft Entra ID Premium, Azure Information Protection, and Microsoft Defender for Identity. Standalone Intune Plan 1 licenses are available at approximately USD 8 per user per month, while Intune Plan 2 is offered as a USD 4 per user per month add-on that enables advanced endpoint management, including remote assistance and specialized security configurations. For device-based licensing applicable to shared or kiosk devices, Microsoft provides Intune Device licenses that facilitate management without user-specific assignment –

however, such use cases fall outside the scope of this user-assigned workstation migration blueprint.

Windows 11 Edition Considerations

Feature/Capability	Windows 11 Pro	Windows 11 Enterprise
MDM Enrollment	✅ Supported	✅ Supported
CSP Support	✅ Most CSPs	✅ All CSPs
Security Baselines	✅ Supported	✅ Full Support
BitLocker Management	✅ Basic	✅ Advanced
Windows Update for Business	✅ Supported	✅ Supported
AppLocker	❌ Not Available	✅ Available
Credential Guard	❌ Not Available	✅ Available
DirectAccess	❌ Not Available	✅ Available

Windows 11 Enterprise edition is recommended for enterprise deployments requiring comprehensive security features and full Configuration Service Provider (CSP) support.

Technical Prerequisites for Migration Initiation

Before initiating migration activities, several technical configurations must be established. The Microsoft Intune subscription should be provisioned within the organization's Microsoft 365 or Enterprise Mobility + Security tenant, with Mobile Device Management (MDM) authority explicitly set to Intune, as opposed to Configuration Manager or third-party solutions. Microsoft Entra ID automatic enrollment must be enabled for relevant user groups, allowing devices to enroll into Intune upon authentication with Entra ID credentials. This setting can be configured via the Microsoft Entra ID administrative portal under the Mobility section, where administrators define the MDM user scope – either universally ("All") or for designated security groups during phased deployments.

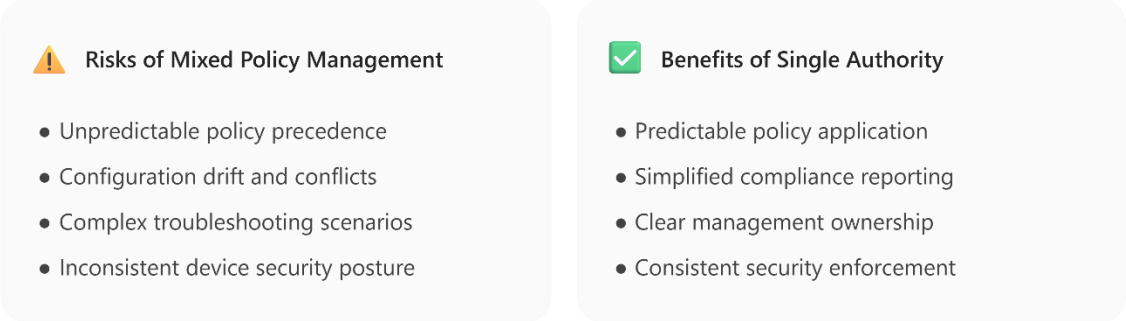
For hybrid Entra ID-joined devices leveraging co-management, a specific Group Policy Object must be implemented within the on-premises Active Directory environment to enable automatic MDM enrollment. This policy, accessible at Computer Configuration > Administrative Templates > Windows Components > MDM, with the setting "Enable automatic MDM enrollment using default Microsoft Entra credentials," ensures that devices enroll in Intune following Group Policy processing. It is also critical to confirm that all Windows 11 devices operate on supported build versions (version 21H2 or newer) to guarantee compatibility with modern management features. Network infrastructure must allow HTTPS traffic to Intune service endpoints, particularly the enrollment discovery URL (https://enrollment.manage.microsoft.com/enrollmentserver/discovery.svc), as this forms the initial contact point during MDM enrollment.

Administrators assigned to oversee the migration process must be granted extensive permissions within both the Microsoft Intune console and the Microsoft Entra ID portal. At minimum, individuals should hold the Intune Administrator role, authorizing them to configure and deploy device profiles, compliance policies, and security baselines. For organizations maintaining Configuration Manager environments during migration, personnel must also possess Full Administrator privileges within Configuration Manager to modify co-management settings and transition workloads from Configuration Manager to Intune.

The Imperative for Policy Separation: Why GPOs and Intune Policies Must Not Coexist

Understanding Policy Conflict and the MDMWinsOverGP Mechanism

A key technical factor influencing migration strategies is the inherent incompatibility between Group Policy Object (GPO) enforcement and Mobile Device Management (MDM) policy enforcement when both seek to configure identical settings on Windows 11 devices. Windows uses distinct engines for processing policies from each configuration method, and unless precedence is explicitly defined, Group Policy settings will override those delivered via MDM in cases of conflict by default. This precedence reflects Windows' legacy architecture, where Group Policy was the principal enterprise configuration tool and MDM support was added later for mobile management needs.



To address this, Microsoft introduced a Configuration Service Provider (CSP) setting that allows administrators to reverse the default precedence. The ControlPolicyConflict/MDMWinsOverGP policy, available in the Policy CSP namespace, can be configured so that MDM-delivered policies take priority over conflicting Group Policy settings. Setting this CSP to "1" ensures that the Windows policy engine prioritizes Intune configurations over GPOs for overlapping settings. Nevertheless, Microsoft's official recommendations advise against relying on this mechanism as a long-term solution, instead suggesting a clear separation of management authorities for consistent and predictable policy application.

Learn about Intune security baselines for Windows devices - Microsoft Intune | Microsoft Learn

The technical justification for avoiding mixed management scenarios extends beyond policy precedence considerations. When devices receive configuration directives from both GPO infrastruc-

ture and Intune MDM policies simultaneously, troubleshooting becomes considerably more challenging, as administrators must assess multiple policy sources to identify which settings ultimately apply. In addition, compliance reporting may become unreliable since Intune dashboards only reflect the MDM policy state and do not account for conflicting GPO configurations that might override intended security measures. From an audit and governance perspective, demonstrating adherence to regulatory frameworks or security standards requires unambiguous evidence of policy application, and mixed management environments complicate the ability to provide definitive compliance verification.

Architectural Reasons for Maintaining Clear Separation

Modern security architectures, such as Microsoft's Zero Trust framework, rely on Conditional Access policies that evaluate device compliance before granting access to corporate resources. These evaluations depend on Intune's capacity to accurately assess device compliance against established baselines and configuration policies. If Group Policy Objects continue to affect device configuration, the compliance status reported to Microsoft Entra ID reflects only Intune-managed components, potentially leading to a misrepresentation of the device's overall security posture where GPOs apply contradictory settings.

Moreover, the cloud-native operational model – considered best practice for enterprise device management – assumes that devices can receive complete configuration updates and policy enforcement without dependence on-premises infrastructure. Continued reliance on GPOs necessitates maintaining connectivity to domain controllers, as policy refresh cycles require periodic access to this infrastructure. This architectural dependency undermines the benefits of cloud-native management, especially for remote workforces whose devices may never connect to corporate networks via VPN. By fully transitioning configuration authority to Intune and separating from GPO-based management, organizations gain the operational flexibility of cloud-based endpoints, ensuring consistent policy enforcement regardless of network location.

Phased Migration Blueprint: From Co-Management to Cloud-Native Intune Management

Phase 1: Environment Assessment and Preparation

The migration initiative begins with a thorough evaluation of the existing Group Policy environment, cataloging all GPOs currently applied to Windows 11 client devices. This inventory should include GPO names, organizational unit (OU) linkages, filtering criteria – such as security group filters and WMI filters – and the specific settings configured within each GPO. It is essential for organizations to distinguish GPOs that address key business requirements from those that enforce legacy configurations potentially no longer relevant. Such assessment forms the basis for migration prioritization, enabling identification of GPOs that must be replicated in Intune versus those suitable for retirement during the transition.

Simultaneously, organizations should review their Configuration Manager (SCCM) infrastructure to document existing co-management workload assignments. This involves determining which

management domains remain under Configuration Manager authority and which have transitioned to Intune. The Configuration Manager console provides visibility of these workload assignments within the Cloud Attach node (or Co-management node in versions 2103 and earlier), indicating whether each workload category is governed by Configuration Manager control, Pilot Intune control (affecting only designated pilot collections), or full Intune control across all co-managed devices.

During this preparatory stage, technical teams should establish an Intune policy framework to supersede Group Policy-based configuration management. This process includes organizing configuration profiles, compliance policies, and security baselines within the Microsoft Intune administrative console. Organizations are advised to define device grouping strategies using Microsoft Entra ID security groups, as Intune policy deployment relies on group-based targeting rather than the OU-centric model employed by Group Policy. This shift from OU-based to group-based targeting constitutes a substantial change, necessitating careful planning to ensure accurate scope and application of policies.

Phase 2: Establishing the Intune Security Baseline Foundation

Microsoft offers pre-configured security baseline templates within Intune, developed by Microsoft's security engineering teams in partnership with the Windows security product group. These baselines provide a comprehensive set of recommended configurations designed to establish secure device posture in accordance with Microsoft best practices and recognized industry standards, such as the Center for Internet Security (CIS) benchmarks.

The Security Baseline for Windows 10 and later serves as the principal framework for Windows 11 device security configuration under Intune management. As of February 2026, the latest version available is Version 24H2, which aligns with the Windows 11 version 24H2 feature release. This baseline encompasses preconfigured settings covering various security domains, including Administrative Templates policies addressing Control Panel personalization restrictions, MS Security Guide recommendations, MSS (Legacy) security options, network parameters, and numerous other critical configuration areas. Each setting is defaulted to reflect Microsoft's recommended security posture; however, organizations retain the ability to tailor individual settings to suit specific business needs or risk profiles.

Administrators implement security baselines by accessing the Microsoft Intune administrative portal, navigating to Endpoint security, selecting Security baselines, and choosing the appropriate template. The deployment process entails creating a profile instance, adjusting settings as required, and assigning the profile to relevant Microsoft Entra ID security groups targeting Windows 11 devices. Microsoft advises organizations to thoroughly review each baseline’s default settings to ensure compliance with internal security policies and regulatory requirements, noting that while preconfigured defaults embody general best practices, they may necessitate modifications based on unique operational considerations.

Phase 3: GPO Discovery and Analysis Using Group Policy Analytics

Microsoft Intune features an advanced analytical tool designed to streamline migration from Group Policy-based configurations to Intune policy frameworks. Group Policy Analytics offers automated assessment capabilities that systematically evaluate exported GPO XML files to identify which settings can be directly migrated to Intune policies, which require alternative implementation strategies, and which lack an equivalent configuration within Intune. By delivering thorough analysis and recommendations for each GPO setting, this tool significantly reduces the manual effort typically associated with planning GPO-to-MDM migrations.

The Group Policy Analytics workflow begins with exporting GPOs from the existing Group Policy infrastructure. Administrators utilize the Group Policy Management Console (GPMC) on a domain controller or administrative workstation to export GPOs in XML format, preserving all relevant settings within a structured representation suitable for analysis. To perform these exports, administrators access the Group Policy Management Console, right-click the desired GPO object, select "Save Report," and choose XML as the output format. This procedure should be repeated for every GPO identified during the initial assessment phase as eligible for migration to Intune.

Once the GPOs are exported, administrators import the XML files into the Group Policy Analytics feature in the Microsoft Intune administrative console. Accessing this function via the Devices menu under Configuration, then selecting Group Policy analytics, administrators can upload the exported XML files. Upon completion of the import, Group Policy Analytics processes the data and produces a detailed report categorizing each setting according to its migration feasibility, along with tailored guidance for implementation.

Settings are classified into several distinct categories to support effective migration planning. Those marked "Supported" indicate that Intune provides direct equivalents, typically through Settings Catalog profiles or Administrative Template policies. For such settings, Group Policy Analytics supplies links to corresponding Intune configuration options, enabling swift creation of equivalent policies. "Supported with alternative approach" denotes settings that lack a direct counterpart in Intune but can be replicated using alternative mechanisms, such as PowerShell scripts deployed via Intune, custom OMA-URI configurations, or third-party integrations. The "Not supported" designation applies to configurations currently unachievable within Intune, prompting organizations to assess their ongoing necessity or consider compensatory security controls in a cloud-native environment.

Additionally, Group Policy Analytics supports automatic generation of Intune Settings Catalog policies based on analyzed GPOs. This capability expedites migration by translating compatible GPO settings directly into Settings Catalog configurations. Administrators have the opportunity to review and refine the automatically generated policies to ensure alignment with organizational requirements before deploying them to pilot device groups for validation ahead of production rollout.

Phase 4: Replicating Security Compliance Toolkit Configurations in Intune

The Microsoft Security Compliance Toolkit (SCT) is a thoroughly curated suite of security baseline Group Policy Objects created by Microsoft's security engineering teams. It offers detailed security configuration guidance for Windows operating systems, Microsoft Office applications, and other Microsoft products. The toolkit provides GPO baselines for Windows 11 across various feature update versions (24H2, 23H2, 22H2, 21H2), delivering version-specific security recommendations tailored to each release's requirements.

Microsoft Security Compliance Toolkit Guide | Microsoft Learn

Organizations that have traditionally implemented Security Compliance Toolkit Group Policy Objects (GPOs) within their on-premises Active Directory environments must evaluate effective strategies for replicating these security configurations in Intune management frameworks. Microsoft offers two primary methods for adopting Security Compliance Toolkit recommendations within Intune, each presenting distinct characteristics and implementation considerations.

The first method involves leveraging Intune's built-in security baseline templates, which incorporate security recommendations developed by the same teams responsible for the Security Compliance Toolkit GPOs. Microsoft's process ensures consistency between GPO-based baselines distributed through the Security Compliance Toolkit and MDM-based baselines available in Intune, thereby providing organizations with equivalent security guidance regardless of the framework selected. Settings within Intune's Security Baseline for Windows 10 and later (version 24H2) are directly derived from the Windows 11 version 24H2 security baseline in the Security Compliance Toolkit, adapted for delivery via Configuration Service Provider (CSP) mechanisms rather than traditional Group Policy methods.

The alignment between Security Compliance Toolkit GPOs and Intune security baselines enables organizations to confidently deploy Intune's built-in security baseline templates, assured of achieving comparable security posture to that established by toolkit GPO baselines. Administrators should be aware, however, that setting nomenclature and presentation differ between GPO-based and MDM-based implementations; while Group Policy settings utilize familiar names and registry references, Intune security baselines employ CSP naming conventions tailored to the Windows MDM configuration architecture. This variation reflects the underlying technical delivery and does not affect functional outcomes.

The second method for replicating Security Compliance Toolkit configurations entails importing GPO XML files from the toolkit into Group Policy Analytics, as outlined in Phase 3, and utilizing automated Settings Catalog policy generation to create Intune policies that closely mirror the original GPO configurations. This approach allows granular control over individual settings and helps organizations maintain exact alignment with specific values defined in the Security Compliance Toolkit, especially where documented adherence is required. However, it necessitates more extensive manual review and validation to ensure that the resulting CSP-based implementations faithfully replicate the intent of the original GPO settings.

Phase 5: Creating Intune Configuration Profiles Using Settings Catalog

The Settings Catalog serves as Intune's most extensive and adaptable configuration profile type, offering access to the complete range of Windows configuration settings provided by Configuration Service Providers (CSPs). In contrast to template-based profiles that deliver a curated selection of commonly used options, the Settings Catalog makes available thousands of individual settings organized by functional category, empowering administrators to build highly tailored profiles aligned with specific organizational needs.

Configuration profiles crafted via the Settings Catalog constitute the principal method for mirroring Group Policy configurations within Intune environments. The catalog interface features a searchable and categorized layout of available settings, each accompanied by comprehensive descriptions, configurable options, and links to pertinent CSP documentation. This breadth of access allows administrators to identify suitable Intune settings for nearly all GPO requirements highlighted during migration assessments, except for certain legacy settings without corresponding MDM capabilities.

To create a Settings Catalog profile, administrators begin in the Microsoft Intune administrative console by navigating to Devices, selecting Configuration, initiating a new policy, choosing Windows 10 and later as the platform, and designating Settings catalog as the profile type. The configuration portal presents settings in a hierarchical structure by domain such as Administrative Templates, Authentication, Browser, Defender, Experience, and other categories. Administrators can browse these domains or utilize the search function to locate settings by name or keyword.

For each setting added to a profile, administrators must define the required configuration value – ranging from enable/disable toggles to numeric, string, or complex multi-value entries depending on specific requirements. The Settings Catalog interface provides controls suited to each setting type, supplemented with clear explanations regarding their purpose and impact. Upon completion of profile configuration, administrators proceed to assignment, selecting Microsoft Entra ID security groups whose devices will receive the profile.

Organizations are advised to adopt a modular approach to Settings Catalog profile architecture, developing distinct profiles focused on individual configuration domains rather than consolidating all settings into large, singular profiles. This strategy streamlines ongoing management by allowing targeted updates to domains without interfering with others, simplifies troubleshooting by isolating conflicts within defined areas, and enhances deployment reliability through avoidance of profile size constraints. Common modularization includes separate profiles for security, networking, application defaults, user experience, and administrative policies.

Phase 6: Transitioning Co-Management Workloads to Intune

For organizations utilizing co-managed Windows 11 devices, in which Configuration Manager and Intune jointly deliver management capabilities, transitioning workload authority from Configuration Manager to Intune marks a pivotal phase in migration. The co-management workload model offers granular control over management domains, enabling organizations to incrementally shift responsibility while assessing Intune policy effectiveness prior to fully decommissioning Configuration Manager.

The transition process is managed via the Configuration Manager console. Administrators can access this by navigating to the Administration workspace, expanding Cloud Services, and selecting the Cloud Attach node (or the Co-management node in Configuration Manager versions 2103 and earlier). Inside the co-management properties dialog, the Workloads tab features slider controls for each workload category. Each slider allows selection among three positions: Configuration Manager (maintaining Configuration Manager authority), Pilot Intune (transitioning authority to Intune for designated pilot collections), or Intune (transferring authority to Intune for all co-managed devices).

Microsoft recommends ensuring comprehensive Intune policy coverage for each workload category before adjusting sliders. Transitioning a workload to Intune without corresponding policies deployed will result in unmanaged devices for that domain, potentially leading to security gaps and operational issues. Consequently, organizations are advised to follow a structured approach: (1) create and validate Intune policies for the relevant workload, (2) deploy these policies to a pilot collection, (3) move the workload slider to Pilot Intune for validation, (4) monitor policy application and compliance, and (5) advance the slider to full Intune upon successful validation.

The typical workload transition sequence begins with Compliance Policies, as these establish device health standards without directly modifying configurations, thereby minimizing operational risk. After successfully transitioning compliance policies, organizations generally proceed to Resource Access Policies (noting their deprecation from Configuration Manager version 2203 onward), then Endpoint Protection, Device Configuration, Windows Update Policies, Office Click-to-Run Applications, and finally Client Apps management. This order reflects an incremental risk strategy, starting with less disruptive workloads and deferring complex application management until Intune policy frameworks have been robustly validated through earlier transitions.

Phase 7: Migrating from Hybrid Entra ID Join to Native Entra ID Join

The transition from hybrid Entra ID-joined device status to native Entra ID-joined status constitutes a major architectural shift in the migration blueprint. This step eliminates reliance on on-premises Active Directory domain infrastructure and finalizes the move to cloud-native device management. According to Microsoft's official guidance, existing hybrid-joined devices cannot be converted directly to native Entra-joined status via in-place reconfiguration; instead, devices require a reset process that removes their current domain join state and establishes them as natively Entra-joined.

This architectural constraint is rooted in core differences between Windows management of domain-joined and Entra-joined device identities. Domain joining creates cryptographic trust relationships with Active Directory domain controllers and generates security identifiers (SIDs) reflecting domain membership within the local device's security database. In contrast, Entra joining forms a distinct cryptographic trust with Microsoft Entra ID and uses separate authentication protocols, including Cloud Kerberos Trust for access to on-premises resources. The Windows security framework does not support concurrent removal of domain join artifacts and establishment of Entra join artifacts without a full device reset, as attempting such a conversion may compromise security token integrity and authentication processes.

Microsoft advises organizations migrating to native Entra ID join status to adopt a dual-track approach. Track 1 focuses on new device deployments and hardware refresh cycles by provisioning all new Windows 11 devices as natively Entra-joined via Windows Autopilot. This method curtails the proliferation of additional hybrid-joined devices, simplifying future migrations and reducing technical debt. Deployment profiles in Windows Autopilot should specify Entra ID join, ensuring that devices attain a cloud-native identity upon initial setup.

Track 2 pertains to existing hybrid-joined devices, acknowledging that hardware refresh cycles typically span three to four years and are insufficient alone to complete fleet migration within a reasonable timeframe. For these devices, Microsoft recommends using the Windows Backup for Organizations feature, which enables the preservation and restoration of user data, application settings, and desktop personalization during device resets. This capability significantly lessens disruption by maintaining continuity of users' personalized computing environments throughout device identity transitions.

The migration workflow for existing hybrid-joined devices includes several preparatory steps prior to initiating a device reset. Organizations must deploy OneDrive Known Folder Move (KFM) policies via Intune to ensure continuous synchronization of user documents, desktop files, and picture folders to OneDrive cloud storage, thereby safeguarding data during device reset operations. The Windows Backup for Organizations feature should be enabled tenant-wide and deployed through Settings Catalog policies, with adequate time allocated for initial backups – typically several days – to accommodate large datasets and ensure reliability. Devices targeted for migration must have verified Autopilot registration and the correct group tags for applying Autopilot profiles specifying native Entra ID join.

To execute migration, administrators issue a wipe command to the target device from the Microsoft Intune console, selecting the appropriate options to exclude preservation of enrollment state or user data, as these are incompatible with the join state change. The device is then reset and enters the Windows Out-of-Box Experience (OOBE), where it initiates the Windows Autopilot provisioning flow. Users authenticate with their Entra ID credentials, after which Windows Backup identifies available backup instances and presents restoration options. Once backup restoration is complete, Autopilot provisioning concludes, and the device is fully natively Entra-joined, with policies and applications deployed based on assigned Autopilot profiles and group-based policy settings.

Phase 8: Configuration Manager Client Decommissioning

Following the successful migration of all co-management workloads to Intune authority and the completion of native Entra ID join, organizations are positioned to decommission the Configuration Manager client from Windows 11 devices. This transition finalizes the move to cloud-native Intune management and removes the necessity of maintaining dual management systems. As a result, it minimizes the endpoint agent footprint and delivers operational efficiencies and security enhancements through a streamlined management architecture.

Before disabling co-management, validate:

1. ✅ All co-management workloads transitioned to Intune
2. ✅ All devices successfully receiving Intune policies
3. ✅ Configuration Manager no longer deploying active policies to target devices
4. ✅ All applications migrated to Intune or alternative delivery methods
5. ✅ Compliance and security reporting functioning in Intune
6. ✅ Devices are Entra ID-joined (not hybrid Entra ID-joined)

The process of uninstalling the Configuration Manager client may be carried out using various methods based on organizational requirements and technical resources. For instance, an organization can deploy a PowerShell script via Intune that programmatically initiates the Configuration Manager client removal (commonly by executing "CCMSetup.exe /uninstall"). Alternatively, Configuration Manager itself can be leveraged to distribute an uninstall package to endpoints before its full decommissioning. It is imperative to confirm that all critical management functionalities have migrated to Intune prior to client removal, since prematurely uninstalling the Configuration Manager client while workloads remain under its management could result in an unintended loss of control over those systems.

Understanding the Microsoft Security Compliance Toolkit and Intune Security Baselines

Architecture and Composition of the Security Compliance Toolkit

The Microsoft Security Compliance Toolkit (SCT) is recognized as Microsoft's definitive collection of security baseline Group Policy Objects, analytical tools, and supporting documentation tailored to assist enterprise security administrators in establishing and maintaining secure Windows environments. Developed and maintained by Microsoft's security engineering teams in collaboration with the Windows product group, the toolkit draws upon extensive security expertise and practical deployment experience to deliver robust, actionable security guidance.

Key components of the toolkit include security baseline GPO packages for various Windows versions. These packages contain pre-configured Group Policy Objects that implement Microsoft's recommended security configurations for respective Windows releases. As of the latest update, the SCT provides security baselines for Windows 11 (versions 24H2, 23H2, 22H2, and 21H2), earlier Windows 10 editions, and Windows Server operating systems. Each baseline package offers both a domain-joined GPO designed for enterprise environments and a local GPO package suited to standalone or workgroup-joined systems without domain infrastructure.

In addition to these baselines, the toolkit features sophisticated analytical and deployment utilities. The Policy Analyzer enables comprehensive comparison of multiple GPO sets, highlighting redundant settings, internal inconsistencies, and configuration differences across baseline versions or organizational customizations. This tool is especially valuable during migration planning, allowing security teams to evaluate current production GPOs against Microsoft's recommended

baselines to identify gaps or deviations needing remediation. The Local Group Policy Object (LGPO) command-line utility streamlines automated deployment and management of local policy settings, supporting scripted policy application for non-domain scenarios and bulk policy automation.

Comparative Analysis: Security Compliance Toolkit GPOs versus Intune Security Baselines

A key consideration for organizations migrating from GPO to Intune is understanding the relationship between the Security Compliance Toolkit's GPO baselines and Intune's built-in security baseline templates. Microsoft has designed both mechanisms with architectural consistency, ensuring that organizations receive comparable security guidance whether they implement recommendations via traditional Group Policy infrastructure or modern MDM policy delivery.

The settings advised in the Security Compliance Toolkit's Windows 11 GPO baselines are closely aligned with those configured in Intune's Security Baseline for Windows 10 and later templates. This alignment demonstrates Microsoft's commitment to unified security standards, irrespective of management technology. Consequently, deploying Intune security baseline templates effectively establishes the same security posture as the GPO baselines, albeit through distinct technical means.

Nevertheless, several critical differences should be carefully evaluated during migration planning. Firstly, the presentation and nomenclature of settings vary significantly between GPO-based and MDM-based implementations. Group Policy utilizes established administrative template policy names, registry references, and terminology familiar to Active Directory administrators, whereas Intune security baselines employ Configuration Service Provider (CSP) names and structures reflective of the Windows MDM ecosystem. For example, a GPO setting titled "Interactive logon: Machine inactivity limit" is represented differently within Intune security baselines under the "LocalPoliciesSecurityOptions" CSP namespace. As a result, administrators need to invest time in mapping GPO settings to their CSP counterparts. Microsoft's documentation offers references to assist with this process.

Secondly, some settings present in the Security Compliance Toolkit GPO baselines may not have direct equivalents in Intune security baselines, due to limitations within the Windows MDM architecture or gaps in CSP implementation. While Microsoft continually expands CSP coverage, certain GPO settings might lack corresponding MDM configurations at any given time. Group Policy Analytics can help identify these discrepancies during migration assessments, enabling organizations to devise mitigation strategies – whether by employing alternative security controls, deploying configuration scripts via Intune, or accepting managed risk when settings pertain to less critical scenarios.

Thirdly, default value recommendations for specific settings may occasionally differ between GPO and Intune baselines. Variations can arise due to differing product group risk assessments or the enhanced configurability offered by MDM policy delivery compared to traditional GPOs. Microsoft recommends reviewing all default settings within both baseline types to confirm alignment with organizational security policies and operational requirements. Uncritically accepting

default values could inadvertently introduce misconfigurations incompatible with business processes or legacy applications.

Implementing Security Compliance Toolkit Recommendations in Intune Environments

Organizations aiming to replicate Security Compliance Toolkit configurations within Intune environments have access to several implementation strategies, each offering unique advantages in terms of fidelity to toolkit specifications, administrative complexity, and maintenance requirements.

The native security baseline approach entails deploying Intune's built-in Security Baseline templates for Windows 10 and later, with either no or minimal customization to meet organizational needs. This strategy ensures optimal alignment with Microsoft's current security guidance, as these baselines are continuously updated by Microsoft in response to new Windows feature releases and evolving threat scenarios. Organizations adopting this method benefit from streamlined management, as they simply update their deployed baseline profiles when new versions are released, eliminating the need for manual tracking and revision of individual settings.

The Group Policy Analytics conversion approach incorporates the importation of Security Compliance Toolkit GPO XML files into Intune's Group Policy Analytics feature. Automated Settings Catalog policy generation is then used to create Intune policies that closely reflect the toolkit's GPO baseline configurations. This method delivers high transparency regarding implemented settings and facilitates comprehensive audit documentation to demonstrate adherence to the Security Compliance Toolkit's standards. However, it demands considerable administrative oversight, requiring verification of generated policies and ongoing monitoring and manual implementation of updates when new toolkit versions are published by Microsoft.

The hybrid approach integrates both strategies by employing Intune's native security baselines for foundational security measures, complemented by supplemental Settings Catalog policies that address Security Compliance Toolkit requirements not covered by the baseline templates or that necessitate further customization. While this method provides a balance between administrative efficiency and detailed control, it also introduces complexity in distinguishing between baseline-derived and catalog-supplemented configurations.

Tools and Techniques for GPO to Intune Conversion

Group Policy Analytics: Functionality and Operational Workflow

Group Policy Analytics represents the cornerstone tool within Microsoft Intune's GPO migration toolset, providing automated assessment capabilities that dramatically reduce the manual effort traditionally required for evaluating Group Policy compatibility with MDM management frameworks. The tool's analytical engine parses exported GPO XML files to evaluate each configured setting against Intune's available policy mechanisms, categorizing settings by migration feasibility and providing implementation guidance for each evaluated configuration.

Setting categorization:

- ✅ **Supported**: Direct MDM mapping available
- ⚠️ **Supported with caveats**: MDM equivalent exists but may behave differently
- ❌ **Unsupported**: No MDM equivalent
- ⏸️ **Deprecated**: Setting no longer applies

The analytical categorization framework used by Group Policy Analytics organizes settings into clearly defined classifications that inform migration planning and execution. Settings labeled as "Supported" denote a direct correspondence within Intune's policy infrastructure, usually through Settings Catalog profiles or Administrative Template policies that leverage the same underlying Configuration Service Provider (CSP) setting as the original GPO. For such settings, the tool frequently offers direct navigation links to the appropriate Intune configuration interface, streamlining policy creation.

Settings designated as "Supported with alternative approach" signify that although an exact MDM equivalent does not exist for the specific GPO function, comparable outcomes can be achieved using alternative Intune features – such as PowerShell script deployment, custom OMA-URI configurations, or third-party integration solutions.

A key strength of Group Policy Analytics is its automated Settings Catalog policy generation capability. This feature translates eligible GPO settings directly into equivalent Intune Settings Catalog profiles, eliminating the need for manual recreation of each setting. This automation significantly increases productivity, particularly when migrating complex GPOs with numerous individual settings. The resulting policies preserve the original GPO's configuration values while adapting them to align with the appropriate CSP mechanisms in Intune. It is important to note, however, that Microsoft recommends a comprehensive review of automatically generated policies before production deployment, as some translations may require adjustments to account for differences between GPO and MDM processing or to address organization-specific needs not represented in the original GPO configuration.

Leveraging Administrative Templates in Intune

Administrative Templates are a distinct category of Intune configuration profiles designed to emulate the functionality of traditional Group Policy Administrative Templates (ADMX/ADML files) within the MDM management framework. These profiles enable administrators to configure a targeted set of Windows and application settings that were historically managed through Group Policy Administrative Templates, thereby providing a familiar interface for those transitioning from GPO-based environments.

The Administrative Templates profile in Intune organizes settings into a hierarchical structure like the traditional Group Policy Management Console. Categories such as Computer Configuration and User Configuration – and their associated subcategories like Control Panel, Network, System, and Windows Components – mirror established groupings, easing the transition for administrators with significant Group Policy experience by leveraging well-known navigation paradigms.

It is important to note, however, that Intune's Administrative Templates profiles offer only a subset of the capabilities available in legacy Group Policy Administrative Templates. The Windows MDM architecture and CSP framework do not replicate all settings, particularly those associated with older or deprecated Windows components. As a result, while Administrative Templates in Intune are valuable for reproducing common GPO configurations, they may not suffice for complete GPO migration. For broader configuration coverage, the Settings Catalog profile type is recommended and aligns with Microsoft's ongoing strategy for Intune policy development.

Custom Configuration Approaches: PowerShell Scripts and OMA-URI Profiles

For GPO settings without direct counterparts in Intune's declarative policy frameworks, organizations can utilize custom configuration methods that allow for the deployment of specialized Windows configurations. These strategies demand advanced technical proficiency beyond typical Intune policy administration but enable the execution of practically any configuration accessible through scripting or registry modification.

PowerShell script deployment via Intune allows organizations to package custom configuration logic within PowerShell scripts, which are executed on managed devices based on administrator-defined schedules. This method is especially effective for replicating intricate Group Policy Object (GPO) configurations that require conditional logic, multi-step processes, or integration with external systems. Administrators prepare the necessary PowerShell scripts, upload them through the Scripts section within the Devices menu in Intune, and assign the scripts to relevant device or user groups. The Intune management agent on Windows devices then retrieves and runs these assigned scripts, recording execution results that administrators can review in the Intune administrative console to confirm successful application of configurations.

OMA-URI (Open Mobile Alliance Uniform Resource Identifier) custom configuration profiles provide administrators with direct access to the Windows Configuration Service Provider (CSP) infrastructure, facilitating the configuration of settings not available through Intune's standard graphical policy interfaces. Implementing this approach requires in-depth knowledge of CSP structures and syntax, as administrators must manually designate the CSP URI path, data type, and configuration values for each setting. While OMA-URI profiles demand a higher degree of technical expertise compared to standard policy profiles, they offer comprehensive flexibility for accessing the full CSP namespace, including experimental or undocumented options valuable in advanced scenarios. Organizations generally use OMA-URI profiles to address specific edge cases beyond the coverage of standard Intune policies, rather than as a primary strategy for GPO migration.

Policy Validation and Troubleshooting During Migration

Verifying Policy Application on Client Devices

A successful transition from Group Policy Object (GPO)-based to Intune-based management necessitates rigorous validation mechanisms to ensure accurate policy deployment to target devices and proper application of intended configurations. Windows 11 offers several native diagnostic

tools and log sources that allow administrators to verify receipt and application of Intune policies. These diagnostic methods differ significantly from traditional Group Policy troubleshooting processes, such as using gpresult.exe or rsop.msc.

The MDM Diagnostic Report is the principal diagnostic artifact for assessing Intune policy application on Windows devices. This detailed XML report provides comprehensive information regarding device enrollment status, applied policies, configuration settings, compliance evaluations, and any error conditions encountered. Administrators can generate the MDM Diagnostic Report by running `mdmdiagnosticstool.exe -out [output_path]` with elevated privileges. The resulting XML file may be reviewed manually or processed within analytical tools for structured examination. Key sections include enrolled MDM providers, device certificate details, instances of applied policies alongside their configuration values, and records of any errors observed during policy processing.

Event Viewer logs deliver real-time insight into MDM policy processing activities and associated errors. Certain log channels are especially valuable when troubleshooting Intune policy issues. The DeviceManagement-Enterprise-Diagnostics-Provider channel (found at Applications and Services Logs > Microsoft > Windows > DeviceManagement-Enterprise-Diagnostics-Provider > Admin) logs events related to device enrollment, policy synchronization, and configuration application. For instance, Event ID 75 denotes successful automatic enrollment, while Event ID 76 signifies an enrollment failure, accompanied by diagnostic error codes. The Task Scheduler operational log (located at Applications and Services Logs > Microsoft > Windows > Task Scheduler > Operational) documents the execution of the automatic MDM enrollment task, where Event ID 107 marks initiation and Event ID 102 denotes completion.

For direct policy inspection on the device, the Settings application grants end users access to applied Intune policies and device compliance status. Users can navigate to Settings > Accounts > Access work or school, select their organizational account, and choose "Info" to review detailed information about device enrollment, applied policies, and the most recent synchronization timestamp. This interface offers clear visibility into specific policies, their application status, and any errors encountered during policy application.

From an administrative standpoint, the Microsoft Intune admin center offers centralized oversight of policy deployment status across managed devices. Within the Troubleshooting + support section, the Troubleshoot pane allows administrators to select individual users or devices to review policy assignments and application outcomes. This interface indicates which policies target a given device, the current application status for each policy (Success, Error, Pending, Not Applicable), and presents detailed error data for failures. Additionally, the Device configuration area under Devices delivers aggregate reporting on configuration profile deployments, outlining the distribution of devices by Success, Error, Conflict, and Pending states for each active profile, thereby facilitating rapid identification of broader policy application challenges.

Troubleshoot policies and configuration profiles in Microsoft Intune - Intune | Microsoft Learn

Common Migration Issues and Resolution Strategies

During GPO-to-Intune migration initiatives, several recurring categories of issues emerge, each necessitating targeted diagnostic and remediation strategies.

Policy Conflict Scenarios: Devices may encounter conflicting configuration directives from multiple policy sources, particularly during transitional phases when both GPOs and Intune policies coexist. Accurately determining the prevailing policy is vital for effective troubleshooting. The MDM Diagnostic Report provides detailed sections that identify the winning policy source for settings affected by multiple assignments. To facilitate smooth transitions, administrators should implement the ControlPolicyConflict/MDMWinsOverGP CSP setting, which grants Intune policies precedence over GPO configurations in cases of conflict. It is important to note that this is intended as a temporary solution rather than a permanent operational approach.

Enrollment Issues: Devices unable to complete Intune enrollment cannot receive management policies, resulting in potential gaps during migration. Common causes of enrollment failure include insufficient licensing (users lacking required Intune licenses), network connectivity barriers preventing access to enrollment endpoints, certificate validation problems, and lingering artifacts from previous MDM providers within device registries. Resolving these issues typically involves verifying user licensing allocations, ensuring network firewall rules permit traffic to necessary Intune service endpoints, and manually removing outdated registry keys from HKLM\Software\Microsoft\Enrollments as needed.

Settings Not Applying: When policies are successfully delivered but individual settings fail to apply, root causes often include platform applicability mismatches, unmet prerequisites (such as BitLocker policies requiring TPM hardware), or conflicts arising from multiple policies attempting to configure the same setting differently. The Intune admin center's troubleshooting tools highlight policies marked as "Not Applicable" or "Conflict," allowing administrators to review assignment criteria and pinpoint problematic configurations. Remediation steps may involve refining policy assignment filters, creating new device groups with more specific membership characteristics, or consolidating overlapping policies into unified configurations.

Licensing Considerations and Cost Implications

The enterprise adoption of Microsoft Intune for comprehensive Windows 11 device management requires a thorough assessment of licensing options and corresponding cost structures. The Intune licensing model is predominantly per-user, with limited exceptions allowing device-based licensing in specific scenarios such as shared devices. As a result, organizations must secure Intune licenses for each user whose devices require management, irrespective of the number of devices assigned to each user.

Typically, enterprises procure Intune through bundled subscription agreements rather than standalone offerings, as these bundles generally deliver greater value by including complementary services. The Microsoft 365 E3 license incorporates Intune Plan 1, which offers foundational Mobile Device Management (MDM) and Mobile Application Management (MAM) capabilities suitable for standard enterprise needs. Enterprises requiring more advanced features – such as enhanced threat protection, privileged access management, or detailed compliance reporting –

may opt for Microsoft 365 E5, which includes Intune Plan 1 and additional security and compliance enhancements. Notably, Microsoft has announced that Intune Suite features will be integrated into both Microsoft 365 E3 and E5 subscriptions beginning in 2026, broadening available functionality without necessitating separate Intune Suite licensing.

Alternative licensing pathways include the Enterprise Mobility + Security (EMS) E3 and EMS E5 bundles, which combine Intune with Microsoft Entra ID Premium, Azure Information Protection, and Microsoft Defender for Identity. These solutions are especially advantageous for organizations seeking robust identity and information protection in conjunction with device management. For those preferring à la carte options, standalone Intune Plan 1 licenses are priced at approximately USD $8 per user per month, while optional Intune Plan 2 add-ons can be acquired for about USD $4 per user per month, offering advanced functionalities such as remote assistance and specialized configuration tools.

From a financial perspective, transitioning from an on-premises Configuration Manager environment to cloud-based Intune management entails both subscription expenses and potential cost savings stemming from the elimination of infrastructure requirements. Configuration Manager implementations demand significant investments in SQL Server database hosting, site server hardware or virtual machines, distribution points, software update configurations, and the ongoing administrative effort required for maintenance and updates. Intune's cloud architecture removes the need for this infrastructure, potentially counterbalancing subscription costs with reductions in hardware and operational labor. Nevertheless, organizations should factor in transition expenses, including migration project staffing, possible consultant services for planning and execution, and training to enhance IT staff proficiency in Intune administration and modern endpoint management practices.

Migration Timeline and Milestones

Migration timelines from GPO-based management to exclusive Intune administration can differ significantly based on factors such as organizational scale, GPO complexity, the maturity of co-management capabilities, and available technical expertise. For large enterprises, these transitions typically span six to eighteen months, commencing with strategic planning and culminating in the decommissioning of Configuration Manager. Organizations with advanced co-management infrastructures and straightforward GPO implementations may realize shorter migration periods. In contrast, environments featuring complex GPO customizations, numerous legacy applications with unique dependencies, or global operations across multiple regions often require extended timelines to ensure thorough validation and rollback protocols throughout each phase.

A standard migration roadmap for mid-sized enterprises managing between 1,000 and 5,000 Windows 11 devices encompasses several critical stages:

- **Months 1-2:** Discovery and Planning, which involves completing GPO inventories, conducting Group Policy Analytics assessments, designing the Intune policy framework, and selecting pilot device groups.

- **Months 3-4:** Intune Policy Development focuses on deploying security baselines to pilot groups, creating and validating Settings Catalog profiles aligned with critical GPO configurations, and advancing application packaging for Intune distribution.
- **Months 5-7:** Workload Transition entails methodically migrating co-management workloads from Configuration Manager to Intune, starting with lower-risk tasks such as compliance policies, followed by device configuration and application management.
- **Months 8-10:** Pilot Entra ID Join Migration involves converting select device cohorts to native Entra ID join status, accompanied by thorough validation of access to on-premises resources, application performance, and user experience.
- **Months 11-13:** Production Entra ID Join Rollout consists of systematically transitioning the broader device fleet to native Entra ID join, synchronized with business unit schedules to minimize operational impact.
- **Months 14-16:** Configuration Manager Decommissioning covers client uninstallation from migrated devices, infrastructure retirement activities, and migration of remaining workflows dependent on Configuration Manager to alternative platforms.

These timelines are based on the expectation of dedicated project resources, executive sponsorship to support cross-functional collaboration, and manageable technical complexity. For global enterprises with rigorous governance requirements, extensive application portfolios needing compatibility verification, or limited IT capacity, migration schedules may be considerably extended – particularly when migration activities must be coordinated alongside continuous business operations.