

Managing Windows Environments with Group Policy

2026 Modernized Edition — 5-Day Instructor-Led

Based on M55630A, updated to reflect current platform realities and practitioner needs

Executive Summary

This proposal outlines a modernized 5-day delivery of Managing Windows Environments with Group Policy. The course retains the structural integrity and learning objectives of M55630A while updating content that has become outdated, deprecated, or misaligned with how Group Policy is practiced in 2026.

The Group Policy landscape has shifted meaningfully since the original course was authored. Several technologies referenced in the standard outline have reached end of life or been formally deprecated. At the same time, the practitioner reality for most Group Policy administrators has evolved from greenfield design toward hybrid management, inheritance scenarios, and co-existence with Microsoft Intune. This modernized edition addresses both realities: it removes or reframes content that is no longer accurate, and it adds targeted coverage of the tools and decisions that today's Group Policy administrators face daily.

The course is delivered across five days rather than the original four to provide appropriate pacing for adult learners, reasonable time for labs and discussion, and room for the additional Intune-era content without compressing the foundational material. The five-day cadence also allows for depth on troubleshooting and real-world scenarios that the compressed four-day version necessarily skims.

Audience

This course is aimed at IT professionals responsible for implementing, supporting, and troubleshooting on-premises and hybrid compute environments built around Active Directory and Group Policy. It is particularly well-suited to:

- Administrators who have inherited existing Group Policy estates and need to understand, audit, and rationalize them
- IT generalists at mid-size organizations where Active Directory and Group Policy remain primary management tools
- Administrators in regulated industries (government, healthcare, defense, financial services) where on-premises identity and policy management continue to be required for compliance or architectural reasons
- Practitioners managing environments in the middle of a transition to Microsoft Intune, who need a framework for deciding what stays in Group Policy and what moves
- Support professionals and helpdesk leads responsible for diagnosing Group Policy application issues on end-user devices

Prerequisites

Attendees will benefit from:

- Familiarity with Windows client and server administration at a working level
- Basic understanding of Active Directory concepts, including users, groups, and organizational units
- Some prior exposure to Group Policy at any level, even if limited to inherited environments
- Comfort with PowerShell for administrative tasks, at a reading-and-minor-editing level

The course does not assume that attendees have deployed Group Policy from scratch. It explicitly accommodates administrators who have inherited existing Group Policy estates.

Delivery Considerations

This modernized edition reflects an active commitment to keeping the course current against the Microsoft platform as it exists, rather than as it existed when the original materials were authored. Content is reviewed and updated in advance of each delivery to account for platform changes, deprecation announcements, and evolving practitioner patterns.

Where the original course was silent on significant current topics — particularly the Group Policy to Intune modernization conversation — this edition addresses them directly. Where the original course referenced technologies that have since been deprecated or reached end of life, this edition handles them honestly: preserving coverage where legacy environments still require it and accurately representing their current lifecycle status.

The lab environment sourcing described earlier reflects the same practical orientation. Rather than defaulting to a purpose-built Group Policy lab that would isolate the course from the hybrid identity and Intune capabilities modern practitioners work with, this delivery leverages a managed hybrid lab environment that supports both the foundational Active Directory and Group Policy content and the new modernization module. The result is a more realistic and more useful training environment.

Learning Outcomes

On completing this course, attendees will be able to:

- Apply both local and remote management techniques to Windows 11 and Windows Server environments
- Describe Active Directory architecture as it pertains to Group Policy planning and troubleshooting
- Design organizational unit structures that support effective Group Policy delegation and administration
- Plan, implement, and maintain a Group Policy infrastructure aligned with organizational requirements
- Understand Group Policy processing order, scope, and conflict resolution, and apply that understanding to real-world troubleshooting
- Manage applications through Group Policy using current supported mechanisms, and understand the practical positioning of AppLocker, App Control for Business, and Smart App Control
- Configure user environments using Group Policy, with awareness of modern alternatives where legacy technologies have been deprecated
- Implement and manage Group Policy Preferences, including item-level targeting

- Configure security through Group Policy, including account policies, user rights, security options, Windows Defender Firewall, and BitLocker
- Maintain Windows 11 through Group Policy, with current understanding of the Windows Update management landscape
- Use Group Policy Analytics and related tooling to assess existing Group Policy estates for Intune migration candidacy
- Apply a structured approach to diagnosing and resolving Group Policy application issues using current troubleshooting tools

Lab Environment

Lab exercises are delivered through a managed hybrid lab environment provided via a Microsoft Learning Partner infrastructure. The environment is deliberately sourced from a modern hybrid identity course platform rather than a purpose-built Group Policy lab, because it provides capabilities that better serve both the foundational and modernized content in this course.

The lab environment includes:

- A fully licensed Microsoft 365 E5 tenant with Microsoft Intune, available for hands-on use throughout the course
- An on-premises Active Directory Domain Services environment with domain controllers, a member server, and hundreds of synchronized user accounts populated via Microsoft Entra Connect
- Windows 11 client machines in both workgroup and domain-joined configurations
- Full administrative access for object creation: attendees can freely create organizational units, Group Policy Objects, users, groups, and other Active Directory objects without restriction
- Persistent state across the full five-day course: work performed on Day 1 is preserved and continues to be available through Day 5, enabling labs that build on earlier exercises

This sourcing decision delivers several practical advantages over a purpose-built Group Policy lab:

- The populated hybrid environment enables realistic exercises that a clean lab cannot support — analyzing and critiquing existing organizational unit structures, working with real Entra Connect sync behavior, and running Group Policy Analytics against meaningful data on Day 5
- The Microsoft Intune tenant is fully available for the Day 5 modernization module, enabling genuine hands-on Group Policy Analytics work rather than instructor-only demonstration
- The environment is actively maintained against current Microsoft platform state, reducing the risk of outdated portal screenshots or deprecated feature references that are common in static lab builds

One minor operational note: the lab platform's sidebar displays credentials and a lab guide from its original course context. Attendees are directed to use the credentials and exercises provided in the course lab guide (delivered as a PDF) rather than those shown in the lab sidebar. This is addressed in the Day 1 orientation and is a trivial adjustment once noted.

Detailed Module Outline

The outline below preserves the learning architecture of M55630A while reflecting the modernization described above. Time estimates are instructional guidance; the 5-day schedule intentionally provides breathing room beyond the estimates shown.

Day 1 — Foundations, Management Tools, and Active Directory Context

Day 1 establishes the foundation: how to manage Windows environments locally and remotely, and the Active Directory architecture that underpins Group Policy. For audiences with strong existing AD background, the afternoon material compresses naturally.

Module 1: Implementing Local and Remote Management

- Overview of Windows 11 and Windows Server local management tools
- Command-line administration, PowerShell, and PowerShell Remoting
- Remote Server Administration Tools and Remote Desktop
- Windows Admin Center in context: where it fits and where it does not
- Lab: Implementing local and remote management

Module 2: Local Group Policy

- Overview of local Group Policies and the Local Group Policy Editor
- Multiple local Group Policy objects and their application order
- Local processing behavior and the impact of domain-joined status
- Lab: Implementing local Group Policy

Module 3: Administering Active Directory (Foundations)

- Active Directory Domain Services fundamentals: forest, domain, OU, and schema
- Domain controllers, the global catalog, and FSMO roles
- Active Directory replication within and between sites
- Sites, subnets, and domain controller location services
- Lab: Implementing and administering AD DS

Instructors note: This module is the most commonly compressed based on audience composition. Cohorts with experienced AD administrators can treat this as a structured review; cohorts with newer administrators benefit from the full treatment.

Day 2 — Organizational Units, Group Policy Fundamentals, and Infrastructure

Day 2 moves from Active Directory context into Group Policy proper: OU design, the mechanics of Group Policy, and the infrastructure considerations for a well-managed deployment.

Module 4: Working with Organizational Units

- Choosing an OU strategy: administrative delegation, Group Policy application, and inheritance
- OU hierarchy considerations for real-world environments
- Creating OUs and delegating Active Directory permissions
- Lab: Creating and managing OUs

Module 5: Overview of Group Policy

- Introduction to Group Policy and the tools available for managing it
- The Group Policy Management Console and Editor hierarchy
- Group Policy Client service, client-side extensions, and refresh behavior
- Domain-based GPOs, GPO storage, and the policies and preferences distinction
- Creating Group Policy Objects and the role of Starter GPOs
- Lab: Creating a GPO

Module 6: Implementing a Group Policy Infrastructure

- Common GPO management tasks and operational patterns
- Delegating administration of Group Policy
- Administrative templates and the central store
- Change management approaches (including context on AGPM's April 2026 end of life and modern alternatives)
- Lab: Implementing a Group Policy infrastructure

Day 3 — Processing, Applications, and User Settings

Day 3 covers the mechanics that determine how Group Policy actually applies, followed by application management and user environment configuration.

Module 7: Managing Group Policy Processing

- Overview of GPO processing and GPO links
- Processing order, conflict resolution, and loopback policy processing
- Considerations for slow links and disconnected systems
- Modifying GPO behavior: link order, enforcement, block inheritance, and security filtering
- WMI filtering and its practical applications
- Enabling and disabling GPOs and GPO nodes
- Lab: Managing Group Policy processing

Module 8: Managing Applications

- Windows 11 application architecture and current application types
- Deploying applications through Group Policy: what still works, what has moved on
- AppLocker: design patterns and the continued role in existing environments
- App Control for Business (formerly WDAC) as the strategic direction for application control
- Smart App Control and the broader modern application control landscape
- Microsoft Store restriction and the shift toward Winget and Intune for deployment
- Lab: Managing applications

Module 9: Managing User Settings

- User state and user profile architecture
- Folder Redirection: implementation, configuration, and troubleshooting
- Offline Files and the user experience considerations
- Logon and logoff scripts via Group Policy
- Brief coverage of UE-V lifecycle (end of life April 14, 2026) and the current landscape of roaming settings solutions
- Lab: Managing user settings

Day 4 — Preferences, Security, and Windows Maintenance

Day 4 handles the topics most directly tied to day-to-day operational work: preferences, security configuration, and keeping Windows updated.

Module 10: Managing Preferences

- Group Policy Preferences: what they are and how they differ from policies
- Preferences processing and available preference categories
- Configuring preferences across registry, files, drive mappings, and scheduled tasks
- Item-level targeting: the practitioner's tool for conditional configuration
- Lab: Managing preferences

Module 11: Configuring Security

- Account Policies, User Rights Assignment, and Security Options
- User Account Control configuration through Group Policy
- Security templates and the Security Compliance Toolkit
- Modifying domain controller security settings
- Active Directory Certificate Services: PKI management through Group Policy
- Certificate autoenrollment and template management
- Windows 11 security features overview and common network security threats
- Windows Defender Firewall: rule design, profiles, and connection security rules
- Implementing BitLocker through Group Policy, including recovery key management
- Interaction with Microsoft Defender for Endpoint and attack surface reduction considerations
- Lab: Configuring security

Module 12: Maintaining Windows 11

- Windows servicing model and available channels
- Windows Server Update Services: formally deprecated, supported through 2035 via Server 2025, and when it remains the appropriate choice (including disconnected environments)
- Windows Update for Business: current best-practice cloud update management for clients
- Windows Autopatch and Azure Update Manager overview
- Configuring Windows Update settings through Group Policy
- Lab: Maintaining Windows 11

Day 5 — Modern Context, Troubleshooting, and Synthesis

Day 5 is the integration day. It places Group Policy in its current ecosystem context, develops structured troubleshooting skills, and closes with synthesis exercises that reinforce the week's material.

Module 13: Group Policy in the Modern Era (New)

- The current state of Group Policy: what it does well, what has moved elsewhere
- Microsoft Intune as a Group Policy peer: Settings Catalog, Administrative Templates in Intune, and the ADMX relationship
- Group Policy Analytics in Intune: ingesting GPO backups, interpreting migration reports, and planning conversion
- Co-managed and hybrid-joined device behavior: the MDMWinsOverGP precedence model
- The practitioner decision framework: which settings stay in Group Policy, which move to Intune, and why
- Realistic modernization roadmaps for organizations with mature Group Policy estates
- Lab: Running Group Policy Analytics in a live Intune tenant against real Group Policy Objects, interpreting the migration compatibility report, and converting a selected subset of settings to Intune Settings Catalog policies

Module 14: Troubleshooting Group Policy

- Group Policy processing review: consolidating the week's material into a diagnostic mental model
- A structured approach to resolving GPO application failures
- Troubleshooting tools: Resultant Set of Policy, Group Policy operational and event logs, gpresult, and PowerShell-based diagnostic techniques
- Identifying and resolving common Group Policy health issues
- Capstone scenario: applying the full week's material to a realistic inherited environment
- Lab: Managing and troubleshooting GPOs