

Protect Business Continuity by Modernizing Group Policy Environment

Get control of Windows configuration management
on premises, in the cloud, or both

How Come Group Policy Hinders Productivity?

The creation of Group Policy was a huge boon to system administrators back in the day. It provides centralized, fine-grained configuration control over Windows desktops and servers, tied to Active Directory. The variety of settings and flexible targeting later led to significant sprawl, conflicting policies, and misconfigurations. These issues affect business continuity, create security gaps, and complicate proving compliance.

Elevating Group Policy Management to end-to-end configuration governance mitigates these risks. Visibility into current deployments highlights conflicts and streamlines optimization. IT teams can plan, approve, and validate changes before they become effective and roll back to a known-good state if issues arise. In short, Group Policy Modernization is about regaining full control of Group Policy, ensuring it works as intended, and understanding if it makes sense to transition Group Policy management to Intune.

Need help to map out the modernization plan?

Talk to the Configuration Expert.

[Contact Us](#)

Modernizing Group Policy to Ensure Reliability

Whether the organization operates on premises only or in a hybrid IT environment, a predictable yet flexible configuration state ensures operational efficiency. Group Policy modernization brings the following benefits:

- 1. Reliability:** Configuration changes for Windows servers and desktops that are expected to be delivered are delivered. Every time.
- 2. Security:** Tight change control and container delegation prevent threat actors from successfully leveraging GPO as an attack vector.
- 3. Auditability:** Change auditing and alerting on unexpected activity accelerates response to cyberthreats.
- 4. Compliance:** Reports and audit trails prove that the policy applies to endpoints as intended to satisfy auditors.
- 5. Governance:** Full visibility into changes, attestation of GPO ownership, control over approval and deployment processes, confirmation of actual implementation.
- 6. Consistency:** Regardless of whether Azure and Intune are already a part of the IT infrastructure or will become so later, all configurations are consistent and ready to be migrated if necessary.

Modernizing Group Policy: Four Steps



Step 1: Clean Up & Optimize Group Policy

The first step is to get a handle on what an organization has today. GPOs grow organically over the years and naturally sprawl, so do Intune profiles. Inventory and assessment of the existing environment help restore the basics, like getting a list of applied GPOs and understanding their settings. Leveraging this knowledge, it becomes possible to get rid of duplicates and conflicts. This phase is especially essential if there is a goal of moving to Intune, as it ensures proper deployment and helps avoid operational disruption.



[GP Reporting Pak](#) automates inventory and analysis to help design the optimized structure with reduced repetition and conflicting configurations. [GPO Migrator](#) facilitates the deployment of desired changes across the IT environment, both on premises and in the cloud. This step alone will significantly boost the operational productivity and resilience of the IT architecture and prepare an organization to migrate to Intune if necessary.

Ready to see them in action?

[Book a demo](#)

Step 2: Manage Change

Once the optimized Group Policy and Intune configurations are in place, it is key to keep them this way:

- Uncontrolled or accidental GPO changes or GPO linking modifications can cause operational outages and affect user productivity.
- Improper GPO or container delegation allows threat actors to compromise GPOs and leverage them to spread malware.
- Uncontrolled Intune profile assignments or profile changes can also cause operational outages and impact users.

Role-based change control addresses these risks by ensuring that changes are reviewed, approved, and deployed by the authorized staff.

[Change Manager for Group Policy/Intune](#) provides role-based change control with editors, approvers, and deployers of GPOs, AD containers, and Intune profiles via a lightweight web-based platform. Immediate or scheduled deployment of changes enables planning updates with minimal impact on users' productivity. Rollback of changes to GPOs, containers, and Intune profiles to a known-good state accelerates recovery if issues occur.

Curious how Change Manager can ensure secure and reliable configuration state?

[Learn More](#)

Step 3:

Audit and Certify Your Group Policy Environment

To ensure consistency of the change process and integrity of the optimized configuration state, it is key to prevent further GPO sprawl. It means that changes need to be not only managed but also audited. Visibility into who changed what, when, and why ensures full control over the configuration state, even if Group Policy and Intune management is spread across multiple teams and IT administrators. Additionally, these audit trails delight both internal and external auditors, making compliance straightforward.

In addition to real-time change auditing, [Group Policy Auditing & Attestation](#) provides GPO attestation capabilities. It allows GPO owners to automatically certify, or attest, that their GPOs remain valid and useful in the environment. This feedback mechanism helps IT teams remove unused GPOs and ensure that critical GPOs, such as those used for security hardening, remain configured as needed to do their jobs.

Looking for a way to simplify compliance?
Let us show how we can help

[Learn More](#)

Step 4:

Validate Group Policy Compliance

The final step is to have confidence that the deployed policies are being delivered successfully. To get away from “push and pray” configuration management, where the IT team just hopes the policy was applied, there is a need for endpoint validation that Group Policy is actually doing its job.

[Group Policy Compliance Manager](#) allows the central collection of Group Policy processing health and settings data from all Windows desktops and servers, along with a variety of reporting against that data. The product provides the feedback mechanism that Group Policy has been lacking, and is the critical final step in the Group Policy modernization process.

Ready to modernize Group Policy?
Talk to the Configuration expert

[Contact Us](#)

About SDM Software

Since 2006, SDM Software has been delivering advanced configuration governance solutions that help organizations secure their Windows environments and maintain business continuity both on premises and in the cloud. Solutions cover the full lifecycle of configuration management on Microsoft platforms, including reporting, migration, automation, auditing, change control, recovery, and compliance reporting. As experts in Group Policy and Intune, SDM Software helps optimize the configuration journey on Microsoft platforms for organizations of all sizes